Quantum Correlations and Quantum Key Distribution

Von der Fakultät für Mathematik und Physik
der Gottfried Wilhelm Leibniz Universität Hannover

zur Erlangung des Grades
Doktor der Naturwissenschaften
Dr. rer. nat.

genehmigte Dissertation
von

Dipl. Phys. Torsten Franz

geboren am 21.02.1981, in Braunschweig

2013

Referent:	Prof. Dr. Reinhard F. Werner,	Leibniz Universität Hannover
Korreferent:	Prof. Dr. Andreas Ruschhaupt,	University College Cork
Tag der Promotion:	31.01.2013	

Abstract

The goal of quantum information science is to accomplish tasks that are impossible within classical concepts using quantum systems. This thesis examines settings in which the quantum world can actually go beyond the classical world and considers how certain quantum features can be utilized to perform the task of secure communication using quantum key distribution.

In the first section we report on our study of the quantum steering effect. This effect describes a certain kind of quantum correlation, that is conceptually stronger than entanglement but weaker then the violation of a Bell inequality. We use the steering effect to investigate the non-classical features of bright light beams in the Gaussian regime. In particular, we see that steering, in contrast to entanglement, is directed. We focus on the bi- and tripartite setting and compare our findings to experimental data.

In the second section we focus on the task of quantum cryptography and present a protocol for key distribution using Gaussian quantum states. We show that this protocol is secure against the most general attacks, even when only a finite number of exchanged signals are considered. The main technical tool we use is an uncertainty relation for the smooth min- and max-entropies. We show that a positive key length is achievable using a setup that is experimentally realizable with current technology.

In the third section, we examine a strong form of security in quantum information, namely device independent security. We are interested in finding the origin of this strong form of security and show that it is actually equivalent to the extremality of the observed probability distribution of outcomes. We further introduce an even stronger independence condition called algebraic security and discuss examples.

Keywords: steering effect, quantum key distribution, Gaussian systems

Zusammenfassung

Das Ziel der Quanteninformation ist es mithilfe von Quantensystemen bestimmte Aufgaben zu bewältigen die mit rein klassischen Methoden unmöglich sind. In dieser Arbeit wird untersucht in welchem Sinne die Quantenwelt sich von der alltäglichen, makroskopischen Welt unterscheidet und wie die besonderen quantenmechanischen Eigenschaften zur sicheren Übertragung von Information mithilfe der Quanten - Schlüsselerzeugung genutzt werden kann. Die Arbeit gliedert sich in drei Teile.

Zunächst beschäftigen wir uns mit dem Quanten-Steering-Effekt. Dieser Effekt beschreibt eine spezielle Art der Quantenkorrelation, die stärker ist als Verschränkung, aber gleichzeitig schwächer als die Verletzung einer Bell-Ungleichung. Wir nutzen den Steering-Effekt zur Untersuchung von nicht-klassischen Eigenschafften an hellen Lichtstrahlen im Gaußschen Regime. Insbesondere sehen wir, dass Steering im Gegensatz zur Verschränkung eine gerichtete Eigenschaft ist. Wir interessieren uns hauptsächlich für die Situation mit zwei und drei Parteien und vergleichen mit experimentellen Daten.

Im zweiten Abschnitt geht es um Quantenkryptographie und wir präsentieren ein Protokoll für die Quanten-Schlüsselverteilung mit Hilfe von Gaußschen Zuständen. Wir zeigen die Sicherheit unseres Protokolls gegen allgemeine Attacken, auch unter Berücksichtigung endlicher Schüssellänge. Unser Hauptwerkzeug hierbei ist die entropische Unschärferelation für Min- und Max-Entropien. Wir zeigen dass mit unserem Protokoll eine positive Schlüsselrate unter heute experimentell realisierbaren Bedingungen möglich ist.

Das dritte Kapitel behandelt eine besonders starke Form der Sicherheit, nämlich geräteunabhängige Sicherheit. Wir interessieren uns hierbei für den Ursprung dieser starken Form von Sicherheit und zeigen, dass diese Sicherheit gleichbedeutend mit der Extremalität der beobachteten Wahrscheinlichkeitsverteilung der Messergebnise ist. Wir werden zusätzlich noch eine stärkere Form der Sicherheit einführen, die wir algebraische Sicherheit nennen, und Beispiele diskutieren.

Stichworte: Steering-Effekt, Quanten-Schlüsselerzeugung, Gaußsche Systeme

Contents

1. Introduction

Overview and Contributions

This chapter will give an outline and a non-technical introduction to this thesis. The "lottery example" in section 1.3 has been published in [DFSW10a].

1.1. Outline

This thesis will be concerned with the study of quantum correlations and how certain correlations can be used to perform quantum key distribution. The main part will be divided into three topics: the study of the steering effect, with a focus on the Gaussian regime, the development of a proof of cryptographic security for a protocol using Gaussian states and the study of extremal quantum correlations as well as their connection to device independent security.

This first chapter will be written on an introductory level and its purpose is to give a summary of our results. We will further give an elementary introduction to the history of quantum mechanics, the nature of Bell correlation inequalities and the history of quantum cryptography.

The second chapter will define our terminology and summarize the technical preliminaries. These will cover the basic structure quantum mechanics, the structure of classical models and the formalism of Gaussian systems.

The third chapter will present different aspects of the steering effect. We will explain the definition and connection to other correlation regimes and then focus on the steering effect for bipartite and tripartite Gaussian systems.

In chapter four we will use Gaussian systems in a quantum cryptographical context. We will present a proof of security for a protocol with squeezed vacuum states, that is secure against general attacks and promises a positive key using technology that is currently available. The main tool here will be the application of the entropic uncertainty relation for smooth entropies.

In the fifth chapter we will study device independent cryptography and show that the origin of this strong form of security is connected to the extremality of quantum correlations. In particular we will show that, in an error free scenario, an eavesdropper will not learn anything about the outcomes of the honest parties if and only if the observed correlations are extremal.

1.2. Historical approach to quantum correlations

Since its development about a hundred years ago, quantum physics has become an essential part of our understanding of nature today. Technology and science both use quantum effects routinely and the control of small quantum systems, down to the level of individual systems has has made significant progress. Still, many questions concerning the structure remain open. One line of inquiry within quantum mechanics is concerned with the question, in which way the quantum mechanical description of the world differs from the classical description. When looking back on the historical development of quantum mechanics, this question has been studied from different angles for quite some time and it took more than fifty years before it became clear that there is a quantitative bound that distinguishes all that is possible within classical mechanics from quantum mechanics. Today we call these bounds Bell inequalities after J. Bell who discovered the first inequality of this kind in the 1964[Bel64]. A collection of the work by Bell can be found in [Bel87].

We will now present a short historical overview on the development of quantum mechanics, with focus on the notions of entanglement, steering and Bell inequalities. This naturally does not claim to be a complete account of all contributions but rather a collection of important steps. For a more complete summary we refer to e.g. [Kra90] and [Kum08]. A useful collection of reprints of papers from 1916 to 1926 can be found in [vdW69], a collection of works by Schrödinger can be found in [Sch63].

The development of quantum physics started at the turn of the 20th century with a number of observations that were not explainable in the by then common framework of classical mechanics. One example for this is the black body radiation that had been studied since the work of Kirchhof (ca. 1860) and led to the theory of radiation by M. Plank (1900) where he introduced a fundamental portion of energy that he later called a “Wirkungsquantum”. The second example is the radiation spectrum of elements like hydrogen, that was independently studied by J. Rydberg and W. Ritz (1888) and ultimately lead to the introduction of the atomic model by N. Bohr (1913). The third effect was the frequency dependence of the photoelectric effect discovered by P. Lennard (1902) and discussed by A. Einstein (1905).

During the following years, more experimental evidence was collected and different theoretical models were proposed, but it was not before the midst of the 1920th that a general foundation was developed. This was done through two approaches, namely the development of the matrix mechanics through M. Born, P. Jordan based on work by W. Heisenberg and the development of wave mechanics by E. Schrödinger. Both approaches were shown to be equivalent by Schrödinger shortly after. For a collection of the work by Heisenberg, Born and Jordan see [vdW69], the work by Schrödinger can be found in [Sch63]. This development triggered a phase in physics that is today referred to as the “golden years” of quantum mechan-

ics, in which many of the problems that had been discovered during the previous 50 years could now be solved within this new theory. In 1932 J. von Neumann published a book on the mathematical framework of quantum mechanics that defined the mathematical foundation of the theory for a long time [vN32].

Despite the huge success of quantum theory, some of the basic questions about the nature of these systems had not been properly addressed. Fundamental objects, like Schrödinger's wave function, still lacked a proper interpretation. In 1926 M. Born had shown that the norm-square of a wave function in position representation can be interpreted as the probability density for results of a position measurement. This did not provide any interpretation for the wave function itself. In hindsight, certain concepts that were developed during this early period and based on semi-classical ideas did later not proof useful and today only of interest in the historical context. We shall not repeat these here, but focus on the arguments that later lead to the modern view on quantum physics, the Einstein-Podolski-Rosen paper, which we will in the following simply denote the EPR paper.

Einstein had been one of the founding fathers of quantum theory, most notably due to his work on the photoelectric effect from 1905 that earned him the Nobel price in 1921, but also due to his work on the quantum foundation of the specific heat in metals 1907 [Ein07]. In the 1920th however, Einstein was known to be a "critic" of quantum mechanics. Here, the term critic should not imply that Einstein had in any way doubted the, even at that time experimentally well confirmed predictions of the theory, but rather that Einstein repeatedly asked the question whether quantum mechanics was indeed the "finest" description of nature possible.

An important historical date here is the Solvay conference on physics 1930. The Solvay conferences were a series of conferences that Einstein had attended before (another notable year in this regard is 1927), and had posed different Gedankenexperimente concerned with the nature of quantum physics, which were then solved by N. Bohr. That year he proposed the "Lichtwaage", a device that should be able to precisely measure the energy of a photon at an exactly determined time, which stood in contrast to the time-energy uncertainty relation. For a detailed account of these two conferences we refer to [Kum08].

In short, the experiment consisted of a box with a small hole that could be opened at a given time to allow a single photon to escape the box. The loss of energy from the box could then be determined by simply weighing the box. After a while, Bohr gave a counterargument to Einstein's example stating (put in a simplified way), that due to general relativity, the change of mass inside the box would lead to a different running time of the clock, thus making the joint determination of time and energy with arbitrary precision impossible. By physicists of that time, this was seen as a great victory of Bohr over Einstein and later repeatedly quoted as such.

In 1935 Einstein, N. Rosen and B. Podolski published a paper [EPR35] which

should revolutionize quantum mechanics, although at that time it went seemingly unnoticed within the scientific world. An "answer" to the paper was produced by Bohr, published in the same journal and was considered by many physicists as a reply sufficient to refute Einstein's criticism. An exception to this general trend was Schrödinger supported and further developed Einstein's idea [Sch35b]. A second notable exception was W.H. Furry [Fur36], whose contributions will be described below. Today, we know that even though the EPR paper was not discussed in the physical literature, many physicists of that time were concerned about it, especially since Einstein's reputation lead to a massive echo in the popular press, that even surprised Einstein himself. For a more detailed account on this time and the reaction by other physicists we also refer to [Kum08].

The question that was addressed by EPR was, if the description of nature provided by quantum mechanics was complete, that is, if quantum theory was really the most fundamental theory possible. In physics, many theories were known to be a coarse-grained version of an underlying theory. One example for this is the behavior of gases as described in statistical physics, which can be explained by using the Newtonian theory of motion for the single particle. A second example is the electric current, which can be described with the flow of single electrons. A natural question was, if there exists also such an underlying theory for quantum mechanics.

In the EPR paper, an example was constructed to support the existence of an underlying theory. In order not to be to technical in this first section, we will only give a plaintext explanation using a different wording than used in the original paper, but we shall see examples of states showing the described behavior later in this thesis.

Consider a bipartite state that is divided between a first party, say Alice, and a second party, called Bob. They are allowed to perform quantum measurements, for instance position and momentum. Suppose, what they find is that whenever they both measure the momentum of their systems they coincide, while whenever they measure the position they differ just by a sign. In both cases, if we consider the situation from Alice's perspective, after measuring the position of her system, she will be able to predict with certainty the outcome of a position measurement by Bob, and likewise for the momentum measurement.

If we were observing systems governed by classical physics this would not be surprising, as it just states that the signals traveling to Alice and Bob travel with exactly the same momentum in opposite directions. In quantum mechanics however, this collides with an uncertainty principle, which forbids a joint measurement with arbitrary precision of position and momentum of a particle. One could argue, however, that the example above does not directly violate this principle as Alice can only predict one of Bob's results with certainty, but the contradiction emerges if one sees that the two systems can be arbitrary far apart for this effect. That means that the system on Bob's side is forced to give the correct answer to any of the two ques-

tions without knowing which one was actually posed on Alice's side. This implies, as there is no connection between Alice's and Bob's lab, the outcomes on Bob's side must be preexisting in some form, possibly not accessible by the two.

In the last part of his paper series from 1935 [Sch35a], Schrödinger compared the situation with a teacher and a pupil[1]. Every day the teacher asks the pupil two questions in random order. He observes, that everyday the pupil gives the answer to the first question always correctly, while answers to the second question might be wrong. As the pupil does not know, which question the teacher will ask first on a specific day, the only conclusion the teacher can draw from this is that the pupil actually knows the answers to both questions, but for some unknown reason, tends to forget the answer to the second one having given the first one correctly.

For Schrödinger and Einstein there are in principle two possible consequences from this example: first, the quantum mechanical description of a single particle by its wave function might not be the finest description possible, or second, there is an objective change in the state on Bob's side when Alice preforms her measurement. They both dismissed the second possibility. Schrödinger used the term "steering" for this phenomenon, as is seems as if Alice's measurement would steer Bob's state into either a position or a momentum eigenstate. Einstein called this second possibility later the "spooky action at a distance". In the pupil example above, Schrödinger concludes with the observation, that the process that the teacher compares the correctness of the first answer to a book of solutions will not change the answer given, especially as the answer could be fixed in the pupils notebook.

As noted above, the scientific community did not seem to recognize the novelty and the implications of the EPR example, partly due to an apparent lack of understanding, partly because some physicists accepted that Bohr had found an inconsistency in the EPR argument and thus proven it wrong. Sources of historical documents for this can be found in [Bor69], [Sch49]; for a detailed discussion we refer to [How95].

In 1951 a quantum physics lecture book by D. Bohm was published, which contained a rephrasing of the EPR experiment into experimentally more practical terms [Boh51]. It had been shown by Schrödinger before, that any non commuting pair of quantum observables could produce the steering effect, but it was the work of Bohm to derive a Stern-Gerlach like setup, which was in principle experimentally feasible. In 1957 Bohm and Y. Aharonov further discussed this setup and discussed different approaches for the state of the individual system that might be compatible with the predictions of quantum mechanics [BA57]. This approach is connected to a question that was discussed in [Fur36]. Here the observation was made, that the EPR effect was related to the fact that the state is pure on the joint system, and that

[1] We will describe the situation in our own words.

the contradiction would vanish, if a process existed that would transform the two parts of the EPR system from a pure to a mixed state. Bohm and Aharonov then discussed the existence of such local mixed states in their example situation.

In 1961 finally, J. Bell approached the question from a general point of view. Where Bohm and Aharonov had pointed out that in their setup certain realizations of local states would produce different predictions that are not compatible with the quantum mechanical prediction, Bell considered a situation to test every local classical model, however it might be constructed. We will give a detailed description of classical models in section 2.2 and an example on the construction of Bell type inequalities in the next subsection. With this formulation, it was possible to construct an experimental situation to test, whether quantum mechanics is actually inconsistent with any local classical model, i.e., whether a finer version of quantum mechanics in the sense of Einstein is indeed possible. The original inequality by Bell was later reformulated by J.F. Clauser, M.A. Horne, A. Shimony and R.A. Holt into the form that is commonly used in experiments with qubits today and will be denoted as the CHSH inequality [CHSH69].

The first experimental verification, that the CHSH inequality is violated was performed by A. Aspect in 1982 [AGR82]. In 1980, B.S. Tsirelson [Tsi80] had shown that the CHSH inequality would also have a maximal value when considering quantum physics and could, in principle, also be used to invalidate quantum mechanics experimentally. These kinds of correlations have, however, not been observed until today (c.f. chapter 2.2). In 1989, R.F. Werner considered again the connection between classically correlated states, i.e., mixtures of product quantum states in the sense of [vN32], and the violation of a Bell inequality. In [Fur36] it was noted, that these states could not be used to display the steering phenomenon and thus (as we know today, c.f. section 3.1) not violate any correlation inequality of Bell type. Werner showed, that the inverse implication is not true - there exist states that obey all correlation inequalities of Bell type, but are not a classical mixture of product quantum states [Wer89].

It should also be noted that the concept of the steering phenomenon, which can be seen as the heart of the EPR argument, was not considered for a long time, especially after the discovery of the Bell type inequalities. The modern formulation that we will be using in the following, and the connection to other correlation measures, was given 2007 by H.M. Wiseman, S.J. Jones and A.C. Doherty [WJD07].

1.3. A short story about Bell inequalities - The quantum lottery

We will now present a short story to motivate the reasoning behind Bell type correlation inequalities. This was originally written as part of a popular science introduc-

tion in [DFSW10a] and will be given here in a slightly enhanced way of presentation.

It was a sunny day when Bob, a physicist experienced with Newtonian physics, wandered about the fair. He walked among the roller coasters, had some cotton candy and was pretty much enjoying himself, when he passed a lottery tent that caught his attention. In bright letters above the tent, a sign said that "Honest Eves Lottery" will be the first lottery to allow the customers to check their chances of winning beforehand. Bob was surprised, as he had always thought of lotteries as scams, ripping the people of their money in a quiet obvious fashion. The basic concept of lottery was, that there are two kinds of lottery tickets - wins and losses, of which a customer draws one at random from a big pot of tickets. The ratio between wins and losses, however, is set by the owner of the lottery. In an extreme case, could simply put only losses in the pot and hope that no customer would recognize this. If, on the other hand, the potential customer of the lottery would know about his odds, he could calculate whether the bet was fair, and decide whether he wants to take the risk.

Bob entered the lottery and looked at the prices. One lottery ticket cost 1$, a winning ticket would get the customer 2$ in return. So the lottery would give fair chances, if there was an equal number of wins and losses in the pot. If he could determine the ratio of wins in the pot, he could decide whether he should play. Bob walks over to the counter and asks the girl about the details. On the front of each ticket there are two fields which can be opened and display either a X or a O sign. The ticket wins when the two signs are equal and loses when they are different. To shorten notation, we will assign symbols to the fields, namely front left (FL) and front right (FR). If Bob wants to determine the number of winning tickets, he has to determine the probability how many of the cards show equal sign, so Prob(FL = FR).

If he was allowed to randomly draw a large number of tickets from the lottery bowl and look at the two fields on the front, he could simply determine the ratio of winning to loosing tickets. But the girl at the counter, Eve, says that this would be to simple - if Bob wanted to open both fields on the front, he would have to actually buy the ticket. But there are other ways to determine the correlation he is interested in. The tickets are equipped with two extra fields on the backside (say BL for the left and BL for the right one, see Fig. 1.1(a)). Bob is allowed to draw as many tickets from the bowl free of charge, as long as he does not open both fields on the front. Also, the tickets are designed in a way that whenever a field is opened, the corresponding field on the opposite side of the ticket is blacked out, see 1.1(b). If for example Bob chooses to open FL the field BL is blackened and he will not learn anything about it. In other words, Bob must choose one of three possible tests for each ticket, i.e., he can open either FL and BL, BL and BL or BL and FR. Now Bob starts to think, how this could help him to get a lower bound on Prob(FL = FR), which in turn is equivalent to giving an upper bound on Prob(FL $\neq$ FR).

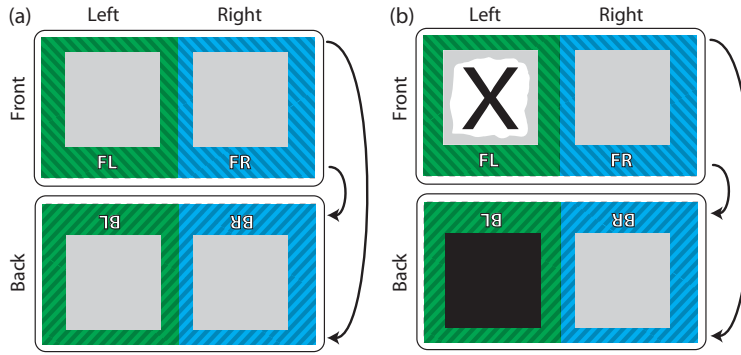

Figure 1.1.: (a) A single lottery ticket. (b) Opening one field on the front will blacken the corresponding field on the back.

The simplest, and most advantageous, case for him would be, if he would always observe correlations in his three test. In this case we would observe three equations, FL = BL,BL = BL and BL = FR, which have to be true at the same time, so the chain of equations FL = BL = BL = FR would tell him that in this case also the values on the fields he is interested in would always have to coincide, i.e., FL = FR. In this case, all tickets in the pot would be winning tickets, so Bob does not expect this to happen. How would the estimation be, if the observed correlations on the test cases are close to maximal? Bob needs to estimate Prob(FL $\neq$ FR), but in all cases where FL $\neq$ FR, the chain of equalities FL = BL = BL = FR has to be broken at least at one point. In this way, when he tests the correlations, any loosing ticket will lead to a different combination of symbols in at least one of his three tests, and he can estimate

$$\text{Prob}(\text{FL} \neq \text{FR}) \leq \text{Prob}(\text{FL} \neq \text{BL}) + \text{Prob}(\text{BL} \neq \text{BL}) + \text{Prob}(\text{BL} \neq \text{FR}). \qquad (1.1)$$

So, Bob begins to draw tickets and determines how often the symbols on the field he checks coincide. To his surprise, his tests reveal that the probability for the symbols he can check to be unequal is roughly 15%. This also means, that the probability that the fields on the front do not coincide is less then 45% and therefore he wins with a probability of at least 55%. Bob is surprised to see that this lottery is not only fair, but gives an advantage to the player. On average, he expects to make a profit of 0.10$ in every round, so he decides to spend his remaining money on lottery tickets. As he opens the tickets, however, he becomes more and more worried as most of his tickets are actually losses - he gets winning tickets with a probability of only 15%. So, poor Bob loses most of his money to Eve and has to end his day at the fair

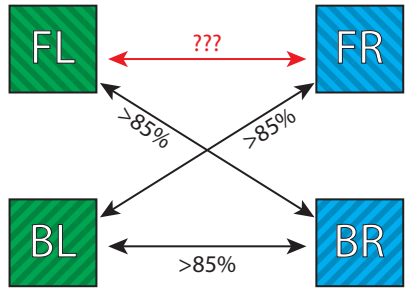

Figure 1.2.: The four fields and correlations observed by Bob. The correlation marked in red is the one he wants to estimate.

earlier as planned.

On his way home, Bob tries to find out, where his reasoning went wrong. After some thought, he concludes, that the only assumption he made in his derivation was, that once he pulls a ticket from the bowl, all symbols in the fields are determined, and opening one field will just reveal a preexisting symbol. If the lottery tickets would on the other hand contain active elements, the observed behavior would be explainable. This would mean that, whenever he opens one of the fields, a signal will travel to the other fields, changing their configuration to match whatever distribution the lottery owner wants the customer to observe. If this was true, it actually would be possible to go beyond the observed numbers - in this case a perfect correlation on the three test configurations would be possible together with a perfect anti-correlation on the winning fields, but probably the owner did not want to make his cheating strategy so obvious.

Feeling pretty smart, Bob returns to the fair the next day to confront Eve with his reasoning and request his money back (maybe with an extra allowance for not telling anybody her trick). To his surprise, Eve is not impressed at all. She says that there is no signal traveling between the left and the right side of the ticket, and that she is willing to make a new bet with him on this. She will sell Bob the whole lottery pot and will give him ten-times his money back if he is able to confirm his claim. Bob agrees, takes the pot and leaves the tent to call a good friend of his, Alice. They meet and decide on a way to check if there is any signal traveling between the sides of the card. To do so, they cut the cards in half, one side is given to Alice and the other side to Bob. They agree on a time at which each ticket should be opened and they will decide at random whether the front or the back should be considered. Any signal that would travel between the half tickets would travel at most at the speed of light, so Alice takes a spaceship to Alpha Centauri to ensure that no signal

from Bob could reach her in time when they open the fields. After meeting back on earth they compare their findings, and if the observed correlations had changed, they would have proven that Eve was using actively communicating lottery tickets. Unfortunately for them, even in this spacelike separated environment the observed correlations do not change.

Now, Bob is out of ideas. He returns to the lottery and begs Eve to reveal her secret to him. Eve gently smiles, and points him towards the nearest quantum mechanics lecture, as the lottery tickets can be realized using quantum mechanical states.

Let us end the story here and discuss, how these lottery tickets are realized in nature. We note that in real life the quantum states realizing the described lottery tickets are way more fragile, but basically all the properties of the tickets can be found in the laboratory. A way of realizing the ticket is the use of polarized light. One could think of a single lottery ticket as been presented by two single photons, one for the left and one for the right side of the ticket. The polarization of the photons can be measured by sending a photon through an analyzer and detect it on a photon counter. If one aligns the analyzer in e.g. the horizontal direction, one can either observe a click of the counter or no click, which corresponds to the two outcome possibilities, i.e., the X or O symbols of the ticket. The two sides of the ticket correspond to the configurations of the analyzer, e.g., horizontal and vertical. Also here the measurement of one will prevent the measurement of the other.

But how can we interpret the results? In the story we have seen that two intuitions from classical physics lead to a contradiction with quantum physics. First is the assumption that every physical system can in principle be described by a list of quantities, and all responses of the system to outside interaction can be determined from this list. In the story, this was the assumption that the symbols on the lottery ticket were determined prior to opening the fields. The second assumption was locality, i.e., that there is no communication between the two sides of the ticket, once they are space like separated. From this it was deduced that the inequality (1.1) has to hold. This in turn also means that any violation of the inequality implies that one of the assumptions is wrong.

The question which of the assumptions has to be dropped, cannot be definitely answered within quantum mechanics, although there are hints. Quantum mechanics as such does not contain any non-local behavior, while the existence of classical parameters is not part of the theory. More severely, however, is the fact that any theory which would drop the locality assumption would stand in contrast to relativity. This is why we, in accordance with most physicists today, subscribe to a statistical interpretation of quantum mechanics. This means that lists of parameters cannot be associated with individual quantum particles. Moreover, this means that quantum mechanics does indeed only describe experiments in a statistical sense, namely, the probability of obtaining certain outcomes in the limit of an infinitely often repeated experiment, but makes in general no prediction about an individual

event.

On the other hand, this does not imply that we need to perform an infinite number of measurements, before we can make predictions. We will see in the following chapters that it is part of a proper description of quantum mechanics to include the estimation procedure in the consideration and to perform the statistical analysis accordingly. Chapter 4 will be concerned with establishing security for a quantum key distribution protocol, where the difficult part exactly is to determine an extractable key from only a finite run of the experiment.

Connection to the CHSH-inequality

In the last section we showed how to derive an inequality for the correlation of bipartite systems under the assumption of an underlying classical model. This inequality is probably the best known Bell type inequality and named the CHSH-inequality [CHSH69]. Usually, this inequality is presented in terms of expectation values of operators and not probabilities, so we will make the connection here. We will use a basic quantum mechanical notation that will be formally introduced in chapter 2.1.

In the lottery story we had considered the probabilities that the symbols on the four possible positions on the tickets do not coincide and derived the following inequality:

$$\text{Prob}(\text{FL} \neq \text{FR}) \leq \text{Prob}(\text{BL} \neq \text{BL}) + \text{Prob}(\text{FL} \neq \text{BL}) + \text{Prob}(\text{BL} \neq \text{FR}). \tag{1.2}$$

To translate this into a quantum mechanical framework, we need to identify the different positions of the ticket with observables. There are four positions, i.e., the front and the back side both either left or right. We want to keep the locality of the two sides for Alice and Bob, so we will say that the two positions on the left are given to Alice and the ones on the right to Bob. Then both will have two observables corresponding to a measurement of the front and back respectively, where we identify the back with the index 1 and the front with the index 2. We further associate the outcome "+1" to the "X" symbol and the outcome "-1" to the "O" symbol. With this, the expectation value for e.g. a joint measurement of the observable A_1 (corresponding to BL) and B_1 (corresponding to BL) is given as

$$\langle A_1 B_1 \rangle = \text{Prob}(\text{BL} = \text{BL}) - \text{Prob}(\text{BL} \neq \text{BL}) = 1 - 2\text{Prob}(\text{BL} \neq \text{BL}). \tag{1.3}$$

The second equality follows, as there are only two outcomes, so $\text{Prob}(\text{BL} = \text{BL}) + \text{Prob}(\text{BL} \neq \text{BL}) = 1$. With these identities for all four combinations we can rewrite (1.2) as

$$\frac{1}{2}(1 - \langle A_2 B_2 \rangle) \leq \frac{1}{2}(1 - \langle A_1 B_1 \rangle) + \frac{1}{2}(1 - \langle A_2 B_1 \rangle) + \frac{1}{2}(1 - \langle A_1 B_2 \rangle) \tag{1.4}$$

which is equivalent to

$$2 \geq \langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + (\langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle , \tag{1.5}$$

i.e., the CHSH inequality in its most common form. One should note here, that the values presented in the story are actually achievable within quantum mechanics. The maximal violation of the CHSH inequality is given by evaluating on state called the maximally entangled qubit state, and gives the value $2\sqrt{2}$ for the right hand side of (1.5). This corresponds to an expectation value of $1/\sqrt{2}$ (resp. $-1/\sqrt{2}$ in the $A_2 B_2$ case) for the individual expectation values. This in turn corresponds to a probability of $\text{Prob}(\text{FL} \neq \text{BL}) = \text{Prob}(\text{BL} \neq \text{BL}) = \text{Prob}(\text{FR} \neq \text{BL}) = (\sqrt{2}-1)/(2\sqrt{2}) \approx 0,146$ and $\text{Prob}(\text{FL} \neq \text{BL}) = (\sqrt{2}+1)/(2\sqrt{2}) \approx 0,853$, so the values given in the story are feasible and can even be exceeded by a small margin.

1.4. A short survey on (quantum-)cryptography and key distribution

The task of cryptography is to enable two or more parties to establish a secure communication. This means, that all messages sent between them cannot be read by an eavesdropper. The question how to establish a perfectly secure way of communicating is of course very old, at least as old as written language. For a popular survey on the different cryptographic methods developed over the ages we refer to [Sin99]. We will not present a historical approach here, but rather focus on the different resources and assumptions used in classical cryptography. We will always use a common terminology in cryptography and name the honest parties in a bipartite setup Alice and Bob, and the eavesdropper Eve.

We start by giving a review on basic principles of classical cryptography. The first is a classification of distribution channels. The main distinction here is between authentic and general channels. The first one allows an eavesdropper to read messages in any way possible but she may not erase or alter messages. If we assume for now that the channel is authentic, the task of secure communication can be seen as a coding problem. In this class of problems, Alice uses a certain scheme, called the encoder, to transform her message into a coded message, also called cypher, which is then transmitted to Bob. We always assume that any classical communication between the legitimate parties is monitored by Eve, so she has a transcript of all messages including the cypher. Bob and Eve now apply a decoding operation to the cypher to reconstruct the original message.

The only way that this is possible for Bob, but not for Eve, is that Bob has some advantage over Eve. One possibility is, that Alice and Bob agree on a specific method of encoding the data that is not known to Eve. An example is the encoding into a

language, or into symbols, that the eavesdropper does not know. This advantage is lost, however, once the eavesdropper gets hold of a translation.

In modern cryptography a clear distinction is made between the method of encryption, which is always assumed to be fully known by Eve, and the pre-shared information which is used as a resource in the communication, commonly called the secret key. This distinction is also called the Kerckhoff principle (see e.g. [Sin99]). In this case the advantage of Alice and Bob over Eve is given by some information that is known only to them, called the cryptographic key. Here, the encryption maps Alice's key and message to the cypher, while the decryption uses Bob's key and the cypher to reconstruct the message. There are two important classes of these key based schemes.

The first one is called a symmetric key scheme, and assumes that the cryptographic key has in some way been distributed to Alice and Bob beforehand. This means that Alice and Bob have to meet in some private setting to agree on a key. Then, whenever they communicate later, they can use the key to encode and decode their communication. In this way the pre-shared key becomes a resource for cryptography, as a key that has been used in some communication cannot be reused for later communication without compromising the security. It is clear, that the quality of the encryption will depend on the length of the key and it can be shown that an encryption scheme can only be perfectly secure if the message and the key have exactly the same length. The most commonly used encryption scheme of this category is the one-time pad (see e.g. [Sin99]).

Unfortunately, the symmetric key system requires that the two communicating parties meet in person, which makes it hardly practical for flexible communication e.g. via the internet. A different approach is asymmetric encryption. The basic principle here is, that Alice and Bob both hold private keys, and use them to generate a third key, called the public key. This public key does not have to be kept secret, but is assumed to be known by the eavesdropper. The actual encryption uses on-way functions. These are functions whose inverse can in the ideal case not be calculated. This means, that the public key can be used to generate the cypher, but it is not enough to perform the decoding. For this, additional knowledge about one of the private keys is required. This asymmetric encryption scheme is standard today in communication over the internet. It should be noted, however, that there are no perfect one way functions, but only functions whose inverse is hard to calculate. Therefore, the security of these systems depends on assumptions on the power of the eavesdropper, i.e., that it is to costly in time and computational power to calculate the inverse function. Schemes which do not rely on such assumptions have also been referred to as "unconditionally secure". This term can be misleading, as it only refers to the eavesdropper's system, and might still impose severe restrictions on the proper working of all devices at Alice's and Bob's side.

As mentioned above, the usage of encodings with a key of sufficient length will

only lead to secure communication once an authentic channel is established. If the eavesdropper is able to delete or manipulate messages, her role in the communication becomes active and new attack strategies arise. If for instance Alice and Bob were to perform an asymmetric protocol without pre-shared information, Eve could intercept all messages and perform a "man in the middle attack", in which she impersonates Bob when talking to Alice and impersonates Alice when talking to Bob. To do so, she establishes a secure communication with Alice using a private key of her own and likewise with Bob. As she decodes the message from Alice and transmits it to Bob, the honest parties will be unaware of Eve's presence, unless they meet in person and compare their cypher messages. This attack can in principle be diminished by using a pre-shared key for authentication, but this would again require that the honest parties meet in person in the first place. When it comes to communicating over the internet, authentication is vital for the security, but not an easy task. If one thinks for instance of online banking, it is necessary for the bank to verify that the customer has the right to access his account, but also the customer has, in principle, to verify that he is talking to his bank and has not been maliciously redirected to some phishing website, that only pretends to be his bank. This authentication over the internet is done using an involved handling of certificates.

Until now, we did not make explicit reference to the signals that are sent between the parties. When we talk about quantum cryptography, however, we always assume that the honest parties are able to exchange quantum signals in addition to classical signals. Quantum cryptography incudes different types of protocols, where we will focus on the probably most common application, namely quantum key distribution (QKD). This task corresponds to the above mentioned scenario where two honest parties want to establish secure communication and will solve the problem of how to establish a key that is secret from the eavesdropper. If such a key is established, classical coding will allow for secure communication as long as the message is not longer than the established key. We note, however, that QKD does not remove the necessity of authentication. For this task, a pre-shared key is still required.

Let us note, that we further assume the laboratories of Alice and Bob being distinct from Eve's laboratory, and that Alice and Bob can seal off their laboratories, if need be. This is important from a conceptual point of view, as every cryptographic scheme would be nullified, if Eve was allowed to hide in Alice's closet or place cameras in Bob's laboratory. There will further be different parts of the equipment that we will assume to be secure. Most prominently, we will allow Alice and Bob access to perfect random number generators. This is an important resource, as the security of every coding scheme relies on the fact that the eavesdropper has no information about the key. We note here that tools from quantum information can also be used for the generation of true random numbers using quantum processes. This

is an own field of research, for an example implementation we refer to [FWN+10].

We will now present a historical overview of quantum key distribution. We will not follow a strict chronological order, but first discuss discrete quantum systems (finite dimensional) and then continuous variable systems (infinite dimensional). For a more detailed survey we recommend [SBPC+09], for a survey on quantum information with Gaussian systems we refer to [WPGP+12].

The first idea of using quantum properties for a cryptographic application dates back to ideas of Wiesner from the 1970th, later published in [Wie84], where he presented an idea of making bank notes secure against counterfeit by implanting a quantum state as a signature. The fact that quantum information cannot be processed, in this case copied, without interaction and thus without disturbance can then be used to detect fraud. At first, his idea did not receive much attention due to the fact that it was technically unpractical. The first practical quantum cryptography scheme was presented in 1984 by Bennett and Brassard, which is today simply called the BB84 protocol [BB84], which was based on the preparation and readout of polarized photons. The first proof of principle was presented shortly after [BBB+92].

In the BB84, Alice prepares states and sends them to Bob, who then measures the states. By comparing the results of Bob's measurements with Alice's preparation, they can infer how much information was lost to the environment in the process and thus to the eavesdropper. This is the prototype of what is called a "prepare and measure" scheme for quantum key distribution. A different concept was put forward in 1991 by A. Eckert, who used a source of highly entangled photons, i.e., photons that maximally violate the CHSH inequality. In this scheme, both Alice and Bob perform measurements and the source of the entangled states can, in principle, be given under the control of the eavesdropper. This type of scheme is also referred to as "entanglement based" scheme. It was shown later that the two schemes are in a certain sense equivalent [BBM92]. In the following years different other schemes have been proposed, using for instance more measurements. For a collection we again refer to [SBPC+09].

For the different protocols, the security has to be proven and different techniques have been developed over the years. In case of the BB84 protocol the first proof goes back to Mayers [May96]. Later proofs were based on entanglement distillation [LC99] or error correction [SP00]. In time different aspects of security have been identified and new security proofs have been developed to include all these aspects. In the first security proofs, the main point was to limit the information of the eavesdropper, that is, to minimize the "accessible information" between Eve and the honest parties. It has been shown [RK05] that this is not a good measure of security, as the key that has been acquired this way can become insecure, when used as part of an encryption scheme. This lead to the development of the notion of composable secure QKD. We will give more technical details about this and the

technical definition of security in chapter 4.

A mayor result was the general proof by I. Devetak and A. Winter that holds for all independent and identically distributed (i.i.d.) sources [DW05]. We call the secret key rate that is acquired using this bound the Devetak-Winter rate (DW-rate), and note that it is applicable to all attacks, in which the eavesdropper performs the same action on every signal. These attacks are also referred to as "collective" attacks, to distinguish them from general attacks, which are also called "coherent" attacks.

The distinction between collective and coherent attacks has only to be considered in one is interested in a finite number of repetitions of the protocol, as in the infinite repetition limit the coherent attacks give no advantage over the collective attacks. In this sense, the DW-rate gives the optimal lower bound of the extractable key rate in this limit. One way of proving this fact is the use of the quantum de Finetti theorem (see [KR05] and references therein). In order to proof security also in the finite key regime one needs to find new proof techniques. The first technique to be both secure against coherent attacks and applicable to finite key analysis was the finite quantum de Finetti theorem for qubit systems [Ren05], which is also composable secure. Later, different proof techniques have been presented, e.g., based on the post-selection theorem [CKR09] or the entropic uncertainty relation [TLGR12].

An issue when considering discrete variable protocols is, that the required hardware is rather specific. For instance, in the original BB84 protocol it was assumed that single photon sources and single photon detectors are available to Alice and Bob. A different approach to QKD is to use bright lightbeams and to use the field quadratures as degree of freedom to transmit the key. The main advantage of these continuous variable (CV) protocols is, that the equipment used, especially the detectors, can be taken from standard telecom components. The first prepare and measure protocol of this type was proposed by Ralph [Ral99], an entanglement based version was presented in [CLA01].

The security analysis for CV protocols on the other hand is more involved, as the security proofs from finite dimensional consideration need to be verified in infinite dimensions. A rigorous proof of for the Devetak-Winter formula in infinite dimension can be derived from [BFS11], further detail can be found in [Fur12]. Also for CV-QKD the asymptotic de Finetti theorem holds, so the DW-rate is asymptotically optimal. The extension of the theorem for finite rounds of the protocol on the other hand, is not directly possible. Even though the de Finetti theorem holds asymptotically, it is actually wrong for any finite number of repetitions [CKMR07]. A technique to truncate the dimension of the Hilbert space to make the finite de Finetti theorem applicable was presented in [RC09], but it was not shown that a positive key rate is possible using this technique is possible when considering realistic parameters. Furthermore in [Ped08] a stability analysis of the technique was performed, but it could not be shown that it is robust against implementation er-

rors. Further approaches have been presented in [GP01, vAIC05] without quantitative analysis. We will present a proof technique that is applicable also for the finite-key regime and is composable secure against general attacks in chapter 4.

When talking about a quantum communication architecture, one should finally not forget, that the QKD part is just one step in the cryptographic protocol. We have noted above, that requirements about the labs still enter the overall security evaluation. In the following we will mainly talk about the QKD part, and not be concerned with the classical communication. When reasoning about the practical value of quantum cryptography this should not be ignored. Especially, device independent key distribution would be for naught, if the classical communication that is performed with the key is itself not trustworthy.

2. Preliminaries

Overview and Contributions

This chapter is devoted to presenting an introduction to the formalism used throughout this thesis. We will describe the formalism of quantum mechanical description for infinite and finite dimensional systems, the notion of a classical model and the formalism of Gaussian systems. Our main motivation is to show that, depending on the specific situation, it is convenient to discuss the quantum system using different frameworks.

We do not claim any novel content here, the chapters purpose is to enhance the self-consistency of the presentation and readers familiar with the subject can safely skip this section.

2.1. Basic quantum systems

We will start by giving a review on the basic formalism of quantum mechanics. For a concise presentation in the language of density operators we refer to [Per95]; for the formalism of general quantum systems we refer to [Haa92].

Quantum mechanics is a statistical theory. Its formalism will allow us to give predictions of measurements that are performed repeatedly on equally prepared systems, which will be explained below. Any experiment consists of a preparation stage and a measurement stage, where the goal of quantum mechanics is to predict the probability of a specific measurement outcome, given a specific preparation.

For completeness we note that in general one could include an intermediate step in the scheme called evolution, in which the state evolved according to some dynamics. But the combination of preparation and time evolution will always form a preparation itself, so we can subsume all time evolution into the preparation. With the same right, it could also be subsumed into the measurement. It is clear, that the physics, i.e., the outcome probabilities, will not be altered by this. The inclusion of the time evolution is also referred to as the "Schödinger picture" while the inclusion in the measurement is called the "Heisenberg picture". For further reading we refer to [Bal98], and note that within this thesis, all time evolution will be part of the preparation.

We will usually be discussing multi-partite situation, i.e., experiments in which different experimenters perform independent measurements. We will also call the experimenters the parties of the experiment and their respective spaces their laboratories. If not stated otherwise, measurement will be performed within a single laboratory, while sources can in general send signals to different laboratories.

We associate to any laboratory a system Hilbert space $\mathcal{H}$ together with collection of possible measurements $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$. This set forms a von Neumann algebra, i.e., a norm-closed $*$-subalgebra of $\mathcal{B}(\mathcal{H})$. For a mathematical introduction to von Neumann algebras and a collection of results, we refer to section A.1 in the appendix and the standard literature [BR79, BR81, Tak02, Haa92]. Let us denote the set of possible outcomes as the measurable set (X, Σ), where Σ denotes a σ-algebra. A specific measurement $F \in \mathcal{M}$ is then described as a positive operator valued measure (POVM) that associates to any subset $x \subset X$ an element $F_x \in \mathcal{M}$. This means we can identify a mapping $A : \Sigma \to M$, and for normalization we set $A(X) = 1$. We will always be interested in measurements with discrete and finite outcome sets, in which case the measurement is defined by a collection of operators $\{F_x\}$ with $\sum_x F_x = \mathbb{1}$. A state will be described as a linear functional $\omega : \mathcal{M} \to [0,1]$, with $\omega(\mathbb{1}) = 1$, such that the probability of observing the outcome result x while using measurement device F is given as

$$\text{Prob}(x|F)_\omega = \omega(F_x). \tag{2.1}$$

We call the set of all states the state space $\mathcal{S}(\mathcal{M})$. Note, that in principle every measurement might come with a different set of possible measurement results. We will try to omit this distinction to keep notation short and always assume that the output space X is large enough to contain all possible outcomes of all measurement if interest. If we want to make the reference to a specific measurement F, we will denote the output set X_F.

In this way, the formalism of von Neumann algebras defines a probability setup in an general way. This formalism can in many practical situations be reduced, namely if the state under consideration is normal. Normal means here, that for all bounded nets of operators $\{F_\alpha\}$ it holds that $\omega(\text{l.u.b.}F_\alpha) = \text{l.u.b.}\omega(F_\alpha)$. Normal states were introduced in [vN49]; for details we refer to chapter 2.4 of [BR79]. For any normal state there exist a density matrix $\rho_\omega \in \mathcal{B}(\mathcal{H})$ with $\text{tr}(\rho) = 1$ such that

$$\text{Prob}(x|F)_\omega = \text{tr}\left(\rho F_x\right). \tag{2.2}$$

This especially implies, that any finite dimensional quantum system can be described in a density matrix formalism. In the following, we will usually identify normal states and their corresponding density matrices.

2.2. Classical models

In the last section we introduced the formalism of quantum mechanics, now we will introduce the concept of a classical model. The motivation for the study of these models lies in the question, to which extend quantum mechanics goes beyond classical physics. We will further introduce Bell inequalities as a tool to distinguish classical models from genuine quantum situations. For reference we refer to the collection of Bell's original papers [Bel87], a collection of results about Bell inequalities can be found in [QIP]. A source for the formalism of statistical theories and quantum mechanics is [Lud83].

The first question we will address in this chapter is, whether it is in principle possible to find a classical description for any quantum effect. To answer this question we need to specify, what we mean by "description". For a specific experiment, the minimal requirement would be that we need to find a statistical model which is compatible with classical physics and is able to reproduce the statistical predictions of quantum theory. If we ask the question in such a general way, the answer is "yes", as we will see below, even if the model constructed this way might be trivial. If we refine the question to also be compatible with the concept of locality, i.e., the possibility of distinguishing different laboratories, the answer will be "no".

A word on terminology: there are different terms in use for the classical models due to historical reasons. Most notable, models are referred to as "hidden variable" models, where the term "hidden" is used to amplify that this model includes parameters that are not part of quantum mechanics, and further more, might not be detectible by any experiment for some underlying physical reason. In the following we will never make explicit reference to whether a classical model contains parts that are explicitly hidden from the observer, so we will use the terms "local hidden variable model" and "classical model" synonymously. As we will further see below, if one allows a classical model without the locality assumption, the question becomes trivial, so we implicitly always assume locality when talking about classical models.

We will again divide the experiment in two parts, the preparation and the measurement, and use the term "source‘" synonymously to "preparation". The preparation will be seen as a black box, whose purpose it is to initialize the system under consideration. In every round of the experiment the system is initialized in a certain configuration λ from a set of possible configurations Λ. This λ contains all information available about the preparation at a specific instant and is in the literature also referred to as the hidden variable. We call a source deterministic, if it will during each run of the experiment output the same configuration, while a general probabilistic source will draw at each instance the configuration with a certain probability, which is given as a probability measure μ. This measure is also

called the statistical state of the system. We emphasize, that we are only interested in experiments that can be performed in a statistical sense, experiments that are unrepeatable are not described by the theory.

The measurement is then the mapping from the configuration to an outcome. Again, we call the measurement deterministic if it returns the same outcome each time it is given the same input, and probabilistic otherwise. Call the set of all measurements $\mathfrak{M}$, a specific choice of measurement device $a \in \mathfrak{M}$ and the set of possible outcome results of this measurement X. Then the measurement is defined by its response function which gives for each outcome and each input the probability of observing the outcome. More specific, it is defined as the probability function $f_a : \Lambda \otimes X \to [0,1]$. It is normalized such that for any configuration one of the outcomes will occur, i.e., $\sum_{x \in X} f_a(\lambda, x) = 1$ for all $\lambda \in \Lambda$. We note, that for many practical applications, the set of possible measurement is given as a parameterized family. For instance, in a typical experiment with polarized photons, any measurement can be described by giving the corresponding parameters in Bloch representation. We will identify the symbol of the measurement with the set of its settings.

Combining the preparation and the measurement, we see that the probability of observing the outcome x while measuring the classical model in the state μ with measurement device a is given as

$$\mathrm{Prob}(x|a)_\mu = \int_\Lambda \mu(\mathrm{d}\lambda) f_a(\lambda, x). \tag{2.3}$$

We will use the symbol $\mathbb{P}$ for such probability distributions and, if clear from the situation, omit the explicit reference to the state, i.e., simply write $\mathbb{P}(a|x)$.

We note here, that in practice one is usually not interested in combining an arbitrary preparation with an arbitrary measurement, but is concerned with a specific situation and only interested in experiments that will give meaningful results. This specific situation, or context, will then define the range of Λ and the structures of possible measurements f_a. We will be only interested in experiments with a meaningful context. We further note that we will consider finite X. In general extension to continuous X and probability densities $\mathbb{P}$ are possible.

A classical model can be transformed into another classical model by renaming the measurement outcomes, or the measurement settings. This implies, that for the study of the structure of such models only the cardinality of X and $\mathfrak{M}$ are of importance. Let us denote the number of settings by $M = (|\mathfrak{M}|)$ and of outcomes as $K = |X|$. In general, the number of outcomes could be different for every measurement, but we can always enlarge a measurement by adding outputs that never occur, so it is no restriction to set the number of outcomes equal. We have considered here a single party experiment, so we denote the set of all probability distributions obeying a classical model in this case as $\mathcal{C}(1, M, K)$.

If two probability distribution $\mathbb{P}_1(x|a)$ and $\mathbb{P}_2(x|a)$ both obey a classical model, then also any convex combination $\alpha\mathbb{P}_1(x|a)+(1-\alpha)\mathbb{P}_2(x|a)$ for $\alpha\in[0,1]$. This can be done by uniting the configuration spaces and drawing either a configuration corresponding to $\mathbb{P}_1$ or $\mathbb{P}_2$ with probability α. As this holds for any probability distribution with classical model, the space $\mathcal{C}(M,K)$ is convex and as such generated by its extreme points. The extreme points of $\mathcal{C}(M,K)$ are exactly the deterministic probability distributions. The proof follows from the above considerations: suppose, $\mathbb{P}$ is extremal, but not deterministic. Then there exists a λ for which at least one response can give two outcomes. But then we can enlarge the model by exactly this random choice, which constitutes a non-trivial convex decomposition which contradicts extremality. Conversely, if $\mathbb{P}$ is deterministic, we can always find a model in which the configuration is directly given as the outcomes. But any decomposition of such a model is necessarily trivial.

We will in the following consider only models with finite M and K, in which case there are only a finite number deterministic probability distributions, namely M^K. Then, $\mathcal{C}(1,M,K)$ is generated by a finite number of extreme points and thus a polytope, which we will also call the classical polytope. With this consideration, we can decide the question whether a probability distributions obeys a classical model by checking, whether it is contained in the classical polytope.

We will show next that the polytope $\mathcal{C}(1,M,K)$ is not enough to distinguish quantum from classical physics, i.e., it is always possible to construct a classical model for any single quantum system. To do so, we note again that a quantum experiment is defined by a state ρ and a set of measurement settings A, where each specific measurement with outcomes from a set χ corresponds to a POVM $F_a=\{F_a(x)\}$ with $\sum_x F_a(x)=\mathbb{1}$. Then the probability of observing outcome x while measuring a is given as $\mathbb{P}(x|a)=\mathrm{tr}(\rho\,F_a(x))$. Please note also that we will restrict to the discussion of normal states.

We will now present two classical models to describe a generic single-party quantum experiment:

In the first model, we choose the space of hidden variables as the set of all quantum states $\Lambda=S(\mathcal{M})$, the state that is produced by the source equal to ω (hence the measure is trivial) and the response function $f_a(\lambda,x)=\omega(F_a(x))$. This model has the same output statistics as the quantum model and caries the description of the quantum state itself as classical variable. This model has a deterministic preparation, as only one configuration is prepared all the time, but defines in general non-deterministic response functions. This means, that there is no way to determine the outcome of a specific event, even if the hidden variable is known.

In the second model, we will choose the space of the classical configurations Λ as $\Lambda=X^{|\mathfrak{M}|}$. Each instance of the hidden variable $\lambda\in\Lambda$ will then be of the form $\lambda=\{x_1,x_2,\ldots,x_{|A|}\}$, where each of the numbers is chosen with probability $\mathrm{Prob}(\lambda_i=x)=\mathbb{P}(x|i)$. Then the response function f_a is simply the function pick-

ing the a-component from λ. Then by definition the outcome probability of the hidden variable model will again equal the quantum mechanical prediction. In this case the model has a non-deterministic preparation but deterministic measurement outcomes. Here, the knowledge of the value of λ in a single run of the experiment would allow the determination of the outcomes of all measurements at the same time.

We note here, that the construction of the second model can also be used to turn an arbitrary classical model into a classical model with deterministic response function. This observation can be useful if one wants to exclude the existence of a general model. It tells us, that the non-existence of a model with deterministic response functions will also exclude any other model.

These previous examples show, that an arbitrary quantum experiment can be described with a classical model, as long as only one system is considered. Next we turn to the bipartite situation. For classical models, the bipartite situation is as follows:

Definition 2.2.1. *For a given bipartite experiment with measurement settings a,b from finite sets of possible measurement settings $\mathfrak{M}_A,\mathfrak{M}_B$ and outcomes x,y from finite sets X_A,X_B we denote the outcome probability distribution by $\mathbb{P}(x,y|a,b)$. We say that this distribution obeys a classical model, if there exist a space of configurations Λ, a probability measure μ and local response functions $f_a:\Lambda\times X_A\to[0,1]$ for $a\in\mathfrak{M}_A$, $g:\Lambda\times X_B\to[0,1]$ for $b\in\mathfrak{M}_B$ such that*

$$\mathbb{P}(x,y|a,b)=\int\mu(d\lambda)f_a(\lambda,x)g_b(\lambda,y). \tag{2.4}$$

We note, that one could also have devised a model with distinct configuration spaces for both sides. But in this case one could always enlarge the space to include both, so this case is included in our definition. Again, the set of all bipartite probability distributions generated by finitely many extreme points and hence again a polytope, which we denote by $\mathcal{C}(2,\vec{M},\vec{K})$. Here $\vec{M}=(M_A,M_B)$ denotes the number of measurement settings for Alice and Bob, where $\vec{K}=(K_A,K_B)$ denotes the number of outcomes. If the number of measurements and outcomes coincide we write $\mathcal{C}(2,M,K)$.

Let us now compare to the structure used within quantum mechanics. We denote the joint Hilbert space of systems A and B as $\mathcal{H}_{AB}=\mathcal{H}_A\otimes\mathcal{H}_B$, the state ρ_{AB} and the measurements F_A and F_B respectively. Then the probability for finding a pair of outcomes x,y given the measurement settings a and b is given as

$$\mathbb{P}(x,y|a,b)=\mathrm{tr}\left(\rho_{AB}F_A\otimes F_B\right). \tag{2.5}$$

We will call the set of all probability distributions with a bipartite quantum model as $\mathcal{Q}(2,M,K)$. It also is a convex set, but in contrast to $\mathcal{C}$ it is no polytope.

We note again, that if we do not need to respect the locality requirement of 3.2, we can always find a classical model in the form 2.3 as

$$\mathbb{P}(x,y|a,b) = \int \mu(\mathrm{d}\lambda) f_{(a,b)}(x,y). \tag{2.6}$$

It is clear, that this polytope $\mathcal{C}(1,M^2,K^2)$ will be larger then the polytope $\mathcal{C}(2,M,K)$ corresponding to 2.5. As an example, if we consider two measurement settings per side and two possible outcomes per measurement, we will in the first case have a polytope with 4^4 extreme points, where in the second case it has only $2^2 \cdot 2^2$. This should certainly not be surprising, as the one party setting does not require locality and hence both outcomes might depend on both settings, where in the bipartite case there is no dependence in the A laboratory on the settings and outcomes in the B laboratory. But this no-signalling principle will actually be even a further distinction. The study of these non-signalling correlations well not be part of our investigation, but we briefly note that all non signalling correlations form a polytope, called $\mathcal{P}$, and there are proper inclusions $\mathcal{C}(2,M,K) \subset \mathcal{P}(2,M,K) \subset \mathcal{C}(1,M^2,K^2)$. For the $M = K = 2$ example, $\mathcal{P}$ has 24 vertices. For further reading we refer to [PBS11] and references given therein.

The above reasoning helped to clarify, under which conditions bipartite quantum probability distributions cannot be modeled with a classical model, namely if $\mathbb{P} \in \mathcal{Q}(2,K,M) \backslash \mathcal{C}(2,K,M)$. We note that the same reasoning also holds for any number of parties $N \neq 1$, i.e., $\mathbb{P}$ is a proper quantum mechanical probability distribution, if it lies in $\mathcal{Q}(N,M,K) \backslash \mathcal{C}(N,M,K)$.

To answer the question, whether a given probability distribution is not-contained in $\mathcal{C}$, one wants to construct appropriate tests. One possibility would naturally be to find a complete parametrization of $\mathcal{C}$, which is in principle possible but nut an easy problem. For further reference we refer to [QIP]. A more natural question is then, whether it is possible to find functions of $\mathbb{P}$ that can certify that $\mathbb{P}$ is not part of $\mathcal{C}$. Such functions are also called witnesses. One type of witness is defined via the faces of the polytope. Every face will give rise to a linear function inequality, and points inside the polytope will fulfil all these inequalities. Conversely, if a single inequality of this type is violated, then the probability distribution is not contained in $\mathcal{C}$. These inequalities will also be called Bell inequalities.

We note, that the nomenclature here is not so strict: also non-linear inequalities, or inequalities that do not correspond to a face of maximal dimension are sometimes called Bell inequalities. We will only consider inequalities corresponding to proper faces in the following.

We have seen, that the classical polytope is generated by a finite number of Bell inequalities. The quantum set $\mathcal{Q}$ is on the other hand not a polytope, but as a convex set generated by its extreme points. The determination of these extreme

points can again be done by optimizing linear functionals, which were introduced by Tsirelson as a quantum analogue to the Bell inequalities and are today called Tsirelson inequalities [Tsi80]. It is clear that any Bell inequality will also define a Tsirelson inequality. These inequalities can be used to distinguish quantum mechanical probability distributions from the aforementioned non-signalling correlations $\mathcal{P}$.

For the $(2,2,2)$-setup the structure is especially simple, as all Bell inequalities are equivalent to the CHSH-inequality [Fin82]. If we call the maximal value of the CHSH-inequality β, it follows that for the classically allowed maximum $\beta_{\mathcal{C}} = 2$, for quantum $\beta_{\mathcal{Q}} = 2\sqrt{2}$, while for non-signalling $\beta_{\mathcal{P}} = 4$.

2.3. Gaussian systems

We will now review the treatment of systems within the Gaussian regime through their Wigner function [Wig32]. For a concise introduction to quantum optics we refer to [WM04], a basic mathematical treatment of unbounded operators with focus on canonical conjugate pairs can be found in [RS78], a good summary of general distribution functions is [HOSW84] and for a review on Gaussian systems with focus on quantum information see [WPGP+12].

We have seen in the previous section that in general quantum systems do not permit a description in familiar classical terms. Especially, if one considers classical physics, the expectation value of any observable f can be described as a configuration space average of the system in state μ as

$$\langle f \rangle_{\mu} = \int \mu(\mathrm{d}\lambda) f(\lambda). \tag{2.7}$$

If one considers the configuration space of the movement of a single particle in one dimension, we can describe its configuration by specifying the position x and momentum p, so the associated Hilbert space will become $\mathcal{L}^2(\mathbb{R}^2)$. In this case, we can reformulate 2.7 by introducing a configuration space density $P_{\mu}(x,p)$ such that

$$\langle f(x,p) \rangle_{\mu} = \int \mathrm{d}x\mathrm{d}p\, f(x,p) P_{\mu}(x,p). \tag{2.8}$$

In quantum mechanics on the other hand, the expectation value of a system in state ρ for an operator F is given as

$$\langle F \rangle_{\rho} = \mathrm{tr}(F\rho). \tag{2.9}$$

We will now review how to derive a description for the behavior of light fields that is similar to the classical configuration space description and works well if mea-

surements of quadrature operators, which will be defined similar to position and momentum, are considered.

This will be done by associating to the system a phase space together with a set of operators, called X and P, that form a canonical conjugated pair. Then we can associate a (quasi-) probability function, called Wigner function W_ρ to the quantum state ρ such that for any quantum mechanical measurement operator $F(X,P)$, which is a Weyl ordered function of the canonical conjugated variables, there exists a classical function $f(x,p)$ such that

$$\langle F\rangle_\rho = \mathrm{tr}(F\rho) = \int \mathrm{d}x\mathrm{d}p\, W_\rho(x,p) f(x,p). \tag{2.10}$$

This formulation was introduced by Wigner in [Wig32] and generalized to all Weyl ordered functions in [Moy49]. For the history of the Weyl order we refer to [Wey50] and [HOSW84].

A single bosonic mode of an optical system can be described with respect to a conjugated pair of unbounded, self-adjoint operators (R_1, R_2), also called field operators, that obey the canonical commutation relation

$$[R_1, R_2] = 2i. \tag{2.11}$$

Here where we note that the value of the constant on the right depends on the chosen scale system, where we choose the convention that the vacuum state will have variance 1, which corresponds to a value $\hbar = 2$. We will associate to each mode space of two real dimensions, which in remembrance of classical physics is also called the the phase space of the system, together with the symplectic form

$$\Sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.12}$$

We will be interested in the detection of quadrature components of the light field, which we will call the amplitude operator $R_1 = X$ and phase operator $R_2 = P$. We note, that in other publications these operators are also designated as position and momentum operator.

In an n-mode system there will likewise be $2n$ field operators, two for each mode, which we will call $\{R_i\}$ with $i = 1...2n$. In this notation the field operators with odd index correspond to amplitude the ones with even index to phase. The symplectic form for the n-mode system is then given by

$$\Sigma = \bigoplus_{k=1}^{n} \Sigma. \tag{2.13}$$

With this, the commutation relation between two field operators is given as $[R_j, R_k] = 2i\Sigma_{(j,k)}$, for $j,k \in \{1,2n\}$.

Consider again a system with n-modes. We denote by $\xi \in \mathbb{R}^n$ a vector in phase space and by $\vec{R} = (R_1, R_2, ..., R_{2n-1}, R_{2n})^T$ the vector of field operators. We define the family of Weyl operators (c.f. [HOSW84]) as

$$W(\xi) = \exp\left(i\xi^T \Sigma \vec{R}\right). \tag{2.14}$$

If one orders the components of the phase space vector accordingly, i.e., $\xi = (p_1, x_1, ..., p_n, x_n)$, this expression becomes

$$W(\xi) = \exp\left(i \sum_i^n (pP - xX)\right), \tag{2.15}$$

and one observes that the operator implements phase space translations. We have now the tools to make the connection between phase space function and the quantum state. Let ρ denote the quantum state, then the characteristic function of the state is given as

$$\chi(\xi) = \mathrm{tr}\left(\rho W(\xi)\right), \tag{2.16}$$

and the Wigner function of the state is given as the symplectic Fourier transform

$$W_\rho(\xi) = \frac{1}{2\pi} \int \mathrm{d}\eta \chi(\eta) \exp(i\eta\Sigma\xi). \tag{2.17}$$

Up to now, the construction has been general and any quantum state has an associated Wigner function. We will now specialize on states with a specific type of Wigner function, namely Gaussian states. Their defining property is, that their Wigner function is Gaussian, i.e., is completely described by its first and second moments.

Definition 2.3.1. *Consider a n-mode quantum system with field operators R_i, $i = 1, ..., 2n$. We call a state ρ a Gaussian state, if its Wigner function is of the form*

$$W_\rho(\xi) = \frac{1}{(2\pi)^n \sqrt{\det(\Gamma)}} \exp\left[-\frac{1}{2}(\xi - \xi_0)^T \Gamma^{-1} (\xi - \xi_0)\right], \tag{2.18}$$

where $\xi_0 = tr\left(\rho \vec{R}\right)$ is the mean expectation vector and Γ with $\Gamma_{i,j} = tr\left(\rho \left\{R_i, R_j\right\}_+\right)$ the covariance matrix.

We will be using the standard nomenclature for Gaussian states, c.f. [WM04].

Definition 2.3.2. *We will call a Gaussian state*

$$\begin{array}{ccccc} \textit{the vacuum state} & & \xi_0 = \vec{0} & & \Gamma = \mathbb{1} \\ \textit{a squeezed vacuum state} & \textit{if} & \xi_0 = \vec{0} & \textit{and} & \Gamma \neq \mathbb{1} \\ \textit{a coherent state} & & \xi_0 \neq \vec{0} & & \Gamma = \mathbb{1} \end{array}.$$

In what will follow, we will always consider vacuum states, and usually in a bipartite setting. In this case, the state is defined by the covariance matrix, which we will write as

$$\Gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{2.19}$$

where the blocks A and B correspond to the subsystems of Alice and Bob and C to the correlations.

Positivity of a state can be expressed in terms of a covariance matrix as follows:

Lemma 2.3.3. *For an N-party Gaussian state it holds*

$$\rho \geq 0 \Leftrightarrow \Gamma + i\Sigma \geq 0. \tag{2.20}$$

The question, whether a state is separable is in general a bit more involved, but if one is only interested to decide separability for a N party setting in a 1 to K split, there is a necessary and sufficient criterion.

Lemma 2.3.4. *A state with covariance matrix γ_{AB} is entangled, if*

$$\gamma_{AB} + \begin{pmatrix} \Sigma & 0 \\ 0 & -\Sigma \end{pmatrix} < 0. \tag{2.21}$$

The covariance matrix is always given with respect to a local choice of basis states. Many interesting properties, such as entanglement and the optimal extractable key rate, do not depend on these choices. One can therefore choose a basis bringing the covariance matrix into a simplified form, the Simon normal form [Sim00]

$$\Gamma = \begin{pmatrix} \lambda_a & 0 & c_x & 0 \\ 0 & \lambda_a & 0 & -c_p \\ c_x & 0 & \lambda_b & 0 \\ 0 & -c_p & 0 & \lambda_b \end{pmatrix}$$

with $\lambda_i \geq c_x \geq |c_p|$. Here c_x and c_p describe the correlations between Alice's and Bob's outcomes of the amplitude and phase measurements. These quantities characterize the state independent of any local basis transformations. However, their dependence on the original (e.g., measured) matrix Γ involves q diagonalization-like process of bringing Γ into this form by suitable local symplectic transformations. It is therefore often easier to use local symplectic invariants with a direct expression in terms of Γ. We use the set [Sim00]

$$I_1 = \det[A] = \lambda_a^2 \tag{2.22}$$

$$I_2 = \det[B] = \lambda_b^2 \tag{2.23}$$

$$I_3 = \det[C] = -c_x c_p \tag{2.24}$$

$$I_4 = \det[\Gamma] = \left(c_x^2 - \lambda_a \lambda_b\right)\left(c_p^2 - \lambda_a \lambda_b\right). \tag{2.25}$$

We will further define some abbreviations: Consider a bipartite Gaussian state ρ_{AB} with covariance matrix Γ. Comparing with 2.19, we call the covariance matrix of the reduced state on Alice's side $\Gamma_A = A$ and the reduced state on Bob's side $\Gamma_B = B$. Without loss, we always call the upper-left entry of any 2×2-submatrix the amplitude quadrature X and the lower right entry the phase quadrature P. If Alice and Bob both perform amplitude measurements, the probability distribution of outcomes will again be a Gaussian distribution with covariance matrix

$$\Gamma_X := \begin{pmatrix} A_{11} C_{11} \\ C_{11}^T B_{11} \end{pmatrix} = \begin{pmatrix} \Gamma_{11} \Gamma_{13} \\ \Gamma_{31} \Gamma_{33} \end{pmatrix}, \tag{2.26}$$

and likewise for the joint phase measurement:

$$\Gamma_P := \begin{pmatrix} A_{22} C_{22} \\ C_{22}^T B_{22} \end{pmatrix} = \begin{pmatrix} \Gamma_{22} \Gamma_{24} \\ \Gamma_{42} \Gamma_{44} \end{pmatrix}. \tag{2.27}$$

3. Einstein-Podolski-Rosen Steering

Overview and Contributions

This chapter reports on our study of Einstein-Podolski-Rosen steering. The theoretical work was performed in collaboration with Jörg Duhme and R.F. Werner in the quantum information theory group in Hannover. The experiments have been carried out in the group of R. Schnabel at the Albert Einstein Institute in Hannover by T. Eberle and V. Händchen in cooperation with S. Steinlechner and A. Samblowski. Results for the have been published in [EHD+11b, EHD+11a] for the two-way situation and in [HES+12] for the one-way situation.

3.1. Introduction and definitions

The concept of steering was introduced by Schrödinger in 1935 as part of a reply to the EPR paper (see section 1.2). The main observation in his example was, that if one interprets the wave function of pure states as the finest possible description of a quantum system, then quantum mechanics contains a process, that does not respect locality. The modern concept of steering was introduced in [WJD07], where it was also shown that it is equivalent to a criterion previously introduced by M. Reid in [Rei89]. For a review on the early years and experimental implementations, we refer to [RDC+09].

There are two approaches to the description of the steering effect. One is based on the formalism of classical models, as introduced in section 2.2 and will allow us to place steering in a correlation hierarchy. The second one is more operational and based on the question whether given states have a common refinement. We will start by giving an example to illustrate the effect in the operational approach. Then we will give the general definition and show the equivalence. Our focus will be on Gaussian systems, and we discuss steering properties for this regime in a bipartite and tripartite scenario.

In what follows, we will always assume that two, or more parties in their respective laboratories perform the experiment, where the laboratories are space-like separated, and that the parties will be named by Alice, Bob and Charlie.

We note, that our definition of steering corresponds to [WJD07], where the ideas of Schrödinger were formalized and the modern definition was given. There ex-

ist a different use of the term "steering" in the literature in connection to so called "steering-ellipsoids", which is based on [Ver01]. Although based on similar considerations, this notion of steering is not equivalent to ours and will not be discussed in what follows.

We start by describing the steering effect for a concrete qubit example. The original argument was made using the EPR state, as given in [EPR35]. We will instead base our description on a pair of maximally entangled qubits, which allow a clearer description.

Let $\rho_{AB} \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be a maximally entangled state. Then the reduced state on Bob's side ρ_B will be maximally mixed, i.e., $\rho_B = \mathbb{1}_2/2$. This state permits an infinite number of decompositions into pure states, i.e., any pair of antipodal points on the Bloch sphere will give such a decomposition. The observation for maximally entangled states is now, that whenever Alice and Bob perform the same projective measurement on their local states, they will always find the same outputs. If Alice performs e.g. a Pauli σ_X measurement and obtains the result $+1$, Bob's conditioned state is also in the $+1$ eigenstate of σ_X. This means that in this case the decomposition corresponding to Bob's local state is in the σ_X basis, and likewise if Alice measures Y in the σ_Y basis. This means that the local state can be decomposed in two ways

$$\rho_B = 1/2|\psi_X^+\rangle\langle\psi_X^+| + 1/2|\psi_X^-\rangle\langle\psi_X^-| = 1/2|\psi_Y^+\rangle\langle\psi_Y^+| + 1/2|\psi_Y^-\rangle\langle\psi_Y^-|, \tag{3.1}$$

where ψ denotes the respective pure eigenstate. This decomposition is now in conflict with the idea that the pure state is the finest description of a single quantum particle. If this was true, then either only one of the decompositions is realized in the specific instance and the choice which one depends on the measurement on Alice's side, or both are realized at every instance. The first possibility conflicts with the space-like separation of Alice and Bob, as the decomposition will take place instantly. The second possibility conflicts with the idea that the pure state is the finest description possible for the individual system.

As noted by Schrödinger in [Sch35b], this contradiction will always occur if the states on Bob's side, conditioned on a specific measurement outcome on Alice's side, are pure. In the same paper he also showed that this property does not change under local unitary dynamics, which is clear when considering the local states at Bob's side in the Bloch sphere representation. If the local states are not pure, however this effect vanishes at some point, as we will show now.

Denote by $\rho_{AB}(w) = w|\psi\rangle\langle\psi| + (1-w)\mathbb{1}/4$, $w \in [0,1]$, a bipartite Werner state [Wer89] where ψ is a maximally entangled state. If we further consider Alice measurement to be either σ_X or σ_Y, the local states on Bob's side will be in the equatorial plane of the Bloch sphere (in a suitable basis). The situation is depicted in Fig. 3.1(a). If the parameter is set to $w = 1$ the four restricted states are pure, hence on the surface of the Bloch sphere. In the parameter is $w = 0$ they are maximally mixed

and coincide in the origin. For any intermediate value, they are equally distant to the origin, the distance given by w. We denote the partial states on Bob's side conditioned that Alice measured in basis $a \in \{0,1\}$ and received outcome $x \in \{+,-\}$ as $\rho^B_{(a,x)}$.

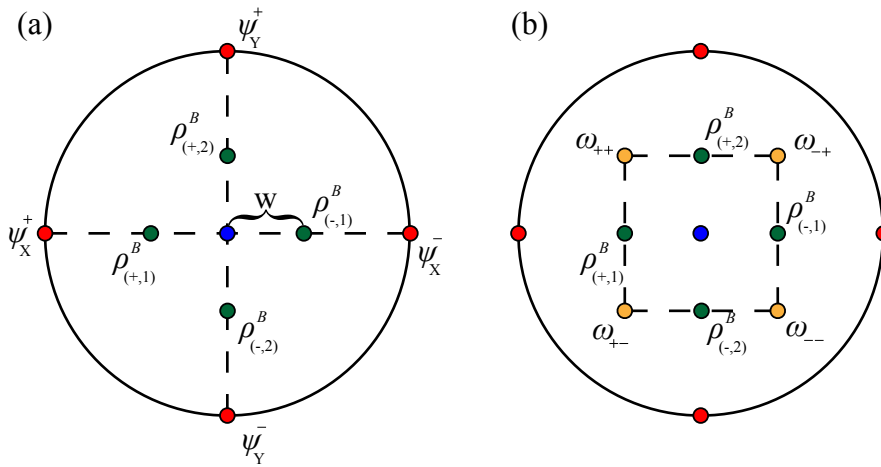

Figure 3.1.: Common refinement for qubits. The circle circle indicates the X-Y plane of the Bloch sphere (a) Reduced states on Bob's side for Werner states corresponding to values 1 (red, pure states), w (green, mixed) and 0 (blue, maximally mixed). (b) A refinement of the states ρ^B into states ω.

A common refinement of the states is found, if there exist states that correspond to outcomes for both possible measurements on Alice's side, which we denote by ω_{x_1,x_2}, where x_1 corresponds to the first and x_2 to the second measurement. This means, there are numbers $p_1, p_2, p_3, p_4 \in [0,1]$ such that

$$\rho^B_{(+,1)} = p_1\omega_{++} + (1-p_1)\omega_{+-} \qquad \rho^B_{(-,1)} = p_2\omega_{-+} + (1-p_2)\omega_{--}$$
$$\rho^B_{(+,2)} = p_3\omega_{++} + (1-p_3)\omega_{-+} \qquad \rho^B_{(-,2)} = p_4\omega_{+-} + (1-p_4)\omega_{--}.$$

In Fig. 3.1(b) we have drawn an example of a common refinement. It is clear, that this common refinement will usually not be unique, except all the refining states are pure and inside the equatorial plane. This corresponds to the maximal case for which a common refinement is possible and will occur at $w = 1/\sqrt{2}$, as can be seen from the construction.

From the previous example we have seen some basic features of steering: a state displays steering, if the states on Bob's side conditioned on measurement on Alice's side do not permit a common refinement. The construction of a common refinement becomes easier the more mixed the local states are.

We will next give a the definition of steering based on the existence of classical models. We recall from section 2.2, that a probability distribution has a classical model, if there exist a parameter space Λ and response functions f, g such that

$$\mathbb{P}(x,y|a,b) = \int \mu(\mathrm{d}\lambda) f_a(\lambda,x) g_b(\lambda,y). \tag{3.2}$$

Let us now define an important subclass of these states, namely those in which the local response functions are realizable within quantum mechanics.

Definition 3.1.1. *A probability distribution obeys a local quantum model on the A side, if there is a Hilbert space $\mathcal{H}_A$, a collection of quantum states $\rho_A(\lambda) \in \mathcal{S}(\mathcal{H}_A)$ and POVMs $F_a = \{F_a^x\}$ such that $f(\lambda,a,x) = tr(\rho_A(\lambda)F_a^x)$.*

A bipartite probability distribution is called separable, if it obeys a local quantum model for both sides, i.e., if it holds that

$$\mathbb{P}(x,y|a,b) = \int \mu(d\lambda) tr(\rho_A(\lambda)F_a^x) tr(\rho_B(\lambda)G_b^y). \tag{3.3}$$

A probability distribution which is not separable is called entangled.

Observe, that the notions of separability and entanglement are commonly defined for states. In the above definition only the states depend on the hidden variable, so we can write

$$\mathbb{P}(x,y|a,b) = \mathrm{tr}(\rho_{AB} F_a^x \otimes G_b^y), \tag{3.4}$$

with

$$\rho_{AB} = \int \mu(\mathrm{d}\lambda) \rho_A(\lambda) \otimes \rho_B(\lambda). \tag{3.5}$$

A state is called separable, if it has such a decomposition into product states. Thus, every separable probability distribution has a realization with a separable state. Conversely it is straightforward to see, that all probability distributions that arise by local measurements of separable states are again separable in the above sense. In the following, we will identify the notion of separability for states and probability distributions when appropriate.

The notion of steerability can now be described in this framework. The distinction between general and separable states has been, that for separable states we can assign a local model that is quantum for both Alice and Bob. The steering property now emerges, if one only makes this requirement for one side.

Definition 3.1.2. *We say that a probability distribution is non-steering from Alice to Bob, if we can find a classical model for Alice's side and a quantum model for Bob's side, i.e., if it holds that*

$$\mathbb{P}(x,y|a,b)=\int \mu(d\lambda) f_a(\lambda,x) tr(\rho_B(\lambda) G_b^y), \tag{3.6}$$

otherwise it its called steering.

We note here, that steering is, in contrast to the existence of a general LHV model or the notion of separability, directed, i.e., we need to distinguish between steering from Alice to Bob and from Bob to Alice. We often omit the explicit mentioning of the direction, if the direction is clear from the context.

$$\begin{array}{ccccc} \text{Bell ineq. violated} & \Rightarrow & \text{Steering} & \Rightarrow & \text{Entanglement} \\ \text{LHV Model} & \Leftarrow & \text{Non-Steering} & \Leftarrow & \text{Separability} \end{array}$$

Figure 3.2.: Sketch of implications.

The three notions (LHV, steering, separability) form a hierarchy, which can be seen from the definitions. If a distribution (or a state) violates at least one Bell inequality, it is steering and if it is steering it is entangled. Conversely, if it is separable it cannot be steering, and if it is not-steering, it has a LHV model. We have summarized the relations in Fig. 3.2.

The natural question now is, whether these implications are actually strict. In the pioneering work [Wer89] a model for qubits was constructed that showed that there exist entangled states which admit a classical model for any projective measurement. This showed that at least one of the implications must be strict. The model constructed there was actually of the form 3.6, thus of the steering type (although this was not mentioned in the paper). In [Bar02] it has been show that there are entangled states admitting a classical model for all POVM measurements on qubits, where the model constructed was not of steering type. We will see below, that all three implications are strict in the Gaussian regime, but for a general setting with arbitrary dimensions and arbitrary measurement, the strictness is not clear.

We will next present a formulation that was derived in [WJD07, CJWR09]. Comparing to the above reasoning about separable states, we note that the requirement on Bob's side corresponds to a restriction on his partial state. Denote by ρ_B the state observed by Bob. Being a quantum state, this state admits different decompositions in purer states of the form $\rho_B = \int \mu(\mathrm{d}x)\rho_x$. This can of course be done for any quantum state and this decomposition is non-unique, unless the state is itself pure, in which case it is trivially non-steering. The notion of non-steering now

requires, that there is in fact a "true" decomposition of the state that corresponds to the local hidden variable $\rho_B = \int \mu(\mathrm{d}\lambda)\rho_\lambda$. This decomposition is in particular independent of the choices and results made on Alice's side. In the literature, this state is also referred to as the local hidden state (LHS).

Finally, we will return to the example from the beginning of the section and define the formalism of common refinements in a general sense.

Corollary 3.1.3. *Bob's local state ρ_B corresponds to a local hidden state, if the states restricted to Alice's settings and outcomes $\rho^B_{(a,x)}$ have a common refinement, where $\rho^B_{(a,x)}$ is the state conditioned on the event that Alice has measured with measurement a and observed outcome x.*

Proof. Suppose, there is a local hidden state. Then we can sort the states in the decomposition of Bob's side according to the outcomes on Alice's. We can in fact make a regrouping with respect to any outcome of all possible measurements on Alice's side, as her side is just classical. Denote by $\underline{x} \in |X|^{|A|}$ the vector corresponding to the output for all measurement settings on Alice's side. Then we have a decomposition of ρ_B as

$$\begin{aligned} \rho_B &= \sum_{\underline{x}} \int \mu(\mathrm{d}\lambda) p(\underline{x}|\lambda)\rho_B(\lambda) && (3.7)\\ &= \sum_{\underline{x}} \rho_B^{\underline{x}}, && (3.8) \end{aligned}$$

where $\rho_B^{\underline{x}} = \int \mu(\mathrm{d}\lambda)p(\underline{x}|\lambda)\rho_B(\lambda)$ denotes the average with respect to the hidden variable. This gives a refinement of the state, as any restriction to a specific result can be recovered by taking the appropriate average

$$\rho^B_{(a,x)} = \sum_{\underline{x},(\underline{x})_a = x} \rho_B^{\underline{x}}, \tag{3.9}$$

where it is important that by construction these states are again proper quantum states.

Conversely, if we have found such a refinement, we know that there exists a local hidden state model, which is just given via this decomposition. Observe, that this common refinement is usually not unique. If the refinement is unique, the refining states are necessarily pure. □

3.2. Steering in the Gaussian regime

We have seen in the previous section, that steering is a quantity that lies in-between separability and the violation of a Bell inequality. In general, these notions do not

have to coincide. In [Wer89] it was first shown, that not all three can be equivalent by giving an explicit classical model that was not separable. Indeed, the model presented was actually a one-sided classical model. In [WJD07], using results from [AGT06], it was shown, that all three notions are strictly different when considering qubit systems and projective measurements. In general, the question is not answered. The first explicit demonstration of the effect experimentally was done in [OPKP92]. For a recent review on the theoretical and experimental progress we refer to [RDC+09].

We are interested in the Gaussian regime, that is, in experiments using Gaussian states and homodyne measurements. Here the notion of steering is a sensible benchmark for experiments. To see this, first note that no experiment in this regime will ever violate a Bell inequality. This follows directly from the definition of Gaussianity: any Gaussian state has a positive Wigner function, which in this case can be interpreted as an outcome probability distribution of values, e.g., for a bipartite system with an outcome vector $\{x_A, p_A, x_B, p_B\}$. The classical hidden variable here is just such an outcome tuple sent to Alice and Bob and response functions that just read out the respective values. Still, there is not always a one-sided classical model. To see this, observe that in the construction the measurement values on both sides were preexisting. This also implies that this model is not necessarily realized by quantum mechanics, e.g., if the measurement operators corresponding to classically joint measurable quantities do not commute.

On the other hand, the Gaussian regime gives a fairly simple criterion for the steering property. This is due to the fact, that all properties of the state can be deduced from its covariance matrix. We start by exploring the definition (3.1.2) in the Gaussian regime. Our formulation is similar to the presentation in [CJWR09]

Theorem 3.2.1. *Consider a Gaussian state ρ_{AB} with covariance matrix*

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \tag{3.10}$$

under Gaussian measurements, so probabilities are given as

$$\mathbb{P}(x,y|a,b) = tr\rho_{AB} W_{a,b}(x,y). \tag{3.11}$$

Then the following conditions are equivalent:

(1) $\mathbb{P}$ is non-steering, i.e. of the form:

$$\mathbb{P}(x,y|a,b) = \int \mu(d\lambda) f_a(\lambda,x) tr(\rho_B(\lambda) G_b^y), \tag{3.12}$$

with $a,b \in \{X,P\}$, G_b Gaussian measurement and $\rho_B(\lambda)$ a Gaussian state.

(2) It holds that

$$\gamma + i\Sigma_B \geq 0. \tag{3.13}$$

where $\Sigma_B = 0 \oplus \Sigma = 0 \oplus \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *denotes the symplectic form on Bob's system.*

(3) There exists a matrix U_B *with*

$$\gamma \geq \begin{pmatrix} 0 & 0 \\ 0 & U_B \end{pmatrix} \quad \textit{and} \quad U_B + i\Sigma \geq 0. \tag{3.14}$$

Proof. We will proof the three implications sequentially.

(1) $\Rightarrow$ (2) Call the measurements under consideration R_a, R_b, where $\{R_a\}$ are the classical observable on Alice's side. Consider an arbitrary combination $X = \sum c_a R_a + \sum c_b R_b,\ c_a, c_b \in \mathbb{C}$. Then, taking the expectation value of X^*X in the given state, and observing that the R_a operators commute with each other and the R_bs, the positivity condition $\langle X^*X \rangle \geq 0$ is equivalent to

$$\left\langle \begin{pmatrix} c_a \\ c_b \end{pmatrix} | (\gamma + \Sigma_B) \begin{pmatrix} c_a \\ c_b \end{pmatrix} \right\rangle \geq 0, \tag{3.15}$$

which gives condition (2).

(2) $\Rightarrow$ (3) We set U_B as the Schur complement $U_B = B - C^T A^{-1} C$. Then from (2) it follows:

$$\begin{aligned}
0 \quad &\leq \quad \inf_{\phi_A \phi_B} \langle \begin{pmatrix} \phi_A \\ \phi_B \end{pmatrix} | (\gamma + i\sigma_B) | \begin{pmatrix} \phi_A \\ \phi_B \end{pmatrix} \rangle \\
&= \quad \inf_{\phi_A \phi_B} (\langle \phi_A | A \phi_A \rangle + \langle \phi_A | C \phi_B \rangle + \langle C\phi_B | \phi_A \rangle + \langle \phi_B | B + i\Sigma_B \phi_B \rangle) \\
&\quad\ \text{Now set } \psi_A = \sqrt{A}\phi_A \\
&= \quad \inf_{\psi_A \phi_B} (\langle \psi_A | \psi_A \rangle + \langle A^{-1/2}\psi_A | C\phi_B \rangle + \langle C\phi_B | A^{-1/2}\psi_A \rangle + \langle \phi_B | B + i\Sigma_B \phi_B \rangle) \\
&= \quad \inf_{\psi_A \phi_B} (\langle \psi_A | \psi_A \rangle + \langle A^{-1/2}\psi_A | C\phi_B \rangle + \langle C\phi_B | A^{-1/2}\psi_A \rangle \\
&\quad\ + \langle A^{-1/2} C\phi_B | A^{-1/2} C\phi_B \rangle - \langle A^{-1/2} C\phi_B | A^{-1/2} C\phi_B \rangle + \langle \phi_B | B + i\Sigma_B \phi_B \rangle) \\
&= \quad \inf_{\psi_A \phi_B} (||\psi_A + A^{-1/2} C\phi_B||^2 - \langle A^{-1/2} C\phi_B | A^{-1/2} C\phi_B \rangle + \langle \phi_B | B + i\Sigma_B \phi_B \rangle) \\
&=^{(*)} \quad \inf_{\phi_B} \langle \phi_B | (B - C^T A C + i\Sigma_B) | \phi_B \rangle
\end{aligned}$$

Where in the last step (*) we used that the minimum of the norm is attained for $\psi_A = -A^{-1/2} C\phi_B$.

With this, condition (1) follows as

$$\langle\phi|\gamma-\begin{pmatrix}0&0\\0&U_b\end{pmatrix}|\phi\rangle=\langle\phi|\gamma-\Sigma_B+\Sigma_B-\begin{pmatrix}0&0\\0&U_b\end{pmatrix}|\phi\rangle \tag{3.16}$$

$$=\langle\phi|\gamma+i\Sigma_B|\phi\rangle-\langle\phi_B|U_B+i\Sigma_B|\phi_B\rangle=0. \tag{3.17}$$

(3)⇒(1) The condition (3) follows via construction of the one-sided classical model. Alice chooses a Gaussian random variable from the distribution with covariance $\gamma-\mathbb{1}\oplus U$ and sends a state with covariance U to Bob. To proof the claim, we need to show that the quantum mechanical expectation value is recovered for all Weil operators:

$$\begin{aligned}\operatorname{tr}\rho_{AB}W(\alpha,\beta) &\overset{qm}{=} \left\langle e^{a\alpha+b\beta}\right\rangle_{\mathbb{P}}\\ &= \int\mu(\mathrm{d}a\,\mathrm{d}b)e^{a\alpha+b\beta}\operatorname{tr}(\rho_B W(\beta))\\ &= \exp\left\langle\begin{pmatrix}\alpha\\\beta\end{pmatrix}\middle|\gamma-\mathbb{1}\oplus U\middle|\begin{pmatrix}\alpha\\\beta\end{pmatrix}\right\rangle\cdot\exp\langle\beta|U\beta\rangle\\ &= \exp\langle\xi|\gamma\xi\rangle\,.\end{aligned}$$

□

This theorem allows us to decide the existence of the classical model by checking the matrix inequality (3.13). This criterion can equivalently be expressed in terms of symplectic invariants:

Proposition 3.2.2. *Let γ be the covariance matrix of a Gaussian state and the syllleptic invariants I_2, I_4 be defined as in 2.22. Then it holds that*

$$\gamma+i\Sigma_B\geq 0\Leftrightarrow\frac{I_4}{I_2}\geq 1. \tag{3.18}$$

Proof. Observe that the positivity is conserved under local symplectic transformations, so without loss, we can consider the matrix γ in Simon normal form. We use the construction via the Schur complement U_B an in 3.2.1. Then one calculates

$$U_B = B-C^TA^{-1}C \tag{3.19}$$

$$= \begin{pmatrix}\lambda_b&0\\0&\lambda_b\end{pmatrix}-\begin{pmatrix}c_x&0\\0&-c_p\end{pmatrix}\begin{pmatrix}1/\lambda_a&0\\0&1/\lambda_a\end{pmatrix}\begin{pmatrix}c_x&0\\0&-c_p\end{pmatrix} \tag{3.20}$$

$$= \begin{pmatrix}\lambda_b-\frac{c_x^2}{\lambda_a}&0\\0&\lambda_b-\frac{c_p^2}{\lambda_a}\end{pmatrix}. \tag{3.21}$$

Note, that we have $\lambda_a\lambda_b \geq c_x^2 \geq c_p^2$, so the trace of U_B is positive and the symplectic positivity is equivalent to the positivity of the determinant, and it holds

$$\begin{aligned} 0 &\leq \det(U_B + i\Sigma) && (3.22)\\ &= \det\begin{pmatrix} \lambda_b - \frac{c_x^2}{\lambda_a} & i \\ -i & \lambda_b - \frac{c_p^2}{\lambda_a} \end{pmatrix} && (3.23)\\ &= (\lambda_b - \frac{c_x^2}{\lambda_a})(\lambda_b - \frac{c_p^2}{\lambda_a}) - 1 && (3.24)\\ &= I_4/I_2 - 1; && (3.25) \end{aligned}$$

which proofs the claim. □

3.2.1. The Reid criterion

The following criterion was proposed by M. Reid in [Rei89]. It is again best understood in terms of the possibility of a local refinement. Suppose, the state is non-steering, then there exists a local refinement in quantum states. In particular, these states do obey the uncertainty relation. If on the other hand an uncertainty relation can be violated when conditioning on certain actions on Alice's side, such a refinement is clearly impossible.

Considering the bipartite situation with Gaussian states and homodyne measurements, the Reid criterion is given as follows:

$$\mathrm{Var}\,(X_b|X_a)\cdot \mathrm{Var}\,(P_b|P_a) \geq 1. \tag{3.26}$$

Here $\mathrm{Var}\,(X_b|X_a)$ denotes the variance of the variable X_b on Bob's side, conditioned on measurement results X_a on Alice's side. The terminology is such that X is called amplitude and P is called phase. One should note that there is no canonical way of assigning these labels to measurement outcomes. In general, this means that the above inequality has to hold for all measurements, if the state is non-steering. On the other hand, a violation for any choice of measurement is enough to certify steering. To see the equivalence to the criteria above, we show that the quantity can be expressed in terms of symplectic invariants.

Proposition 3.2.3. *For a Gaussian state with covariance matrix γ it holds that*

$$Var\,(X_b|X_a)\cdot Var\,(P_b|P_a) = \frac{I_4}{I_2}. \tag{3.27}$$

Proof. First note, that the correlation between Alice and Bob is optimal for measurements whose bases have been chosen such that all diagonal elements in the

sub-matrices vanish. In this case, we can express the covariance matrix as

$$\gamma_{AB} = \begin{pmatrix} \lambda_1 & 0 & c_x & 0 \\ 0 & \lambda_2 & 0 & -c_p \\ c_x & 0 & \lambda_3 & 0 \\ 0 & -c_p & 0 & \lambda_4 \end{pmatrix} \tag{3.28}$$

The conditional variance of, e.g., Bob's X result conditioned on Alice's result is $\mathrm{Var}(X_b|X_a) = \lambda_3(1 - \frac{c_x^2}{\lambda_1\lambda_3})$. With this we can calculate

$$\begin{aligned} \mathrm{Var}(X_b|X_a)\cdot\mathrm{Var}(P_b|P_a) &= \lambda_3\left(-\frac{c_x^2}{\lambda_1\lambda_3}\right)\lambda_4\left(-\frac{c_p^2}{\lambda_2\lambda_4}\right) \\ &= \lambda_3\lambda_4 - \frac{\lambda_3}{\lambda_2}c_p^2 - \frac{\lambda_4}{\lambda_1}c_x^2 + \frac{c_x^2c_p^2}{\lambda_1\lambda_2} \\ &= (\lambda_1\lambda_2\lambda_3\lambda_4 - \lambda_1\lambda_3c_p^2 - \lambda_2\lambda_4c_x^2 + c_x^2c_p^2)/(\lambda_3\lambda_4) \\ &= I_4/I_2 \end{aligned}$$

□

3.2.2. EPR-Steering from a single squeezed source

For the experimental realization of EPR-steering, one needs a sufficiently strong source of entangled light. We report in the following on an entanglement source that is build up by a single source of squeezed light, which is entangled with a vacuum mode forming vacuum class, or short v-class, entanglement. We will present data obtained from a measurement that was published in [EHD+11b], which was to our knowledge the first reported observation of v-class steering. We note that in more recent experiments, e.g. [EHD+11a], even higher levels of steering from v-class entanglement have been observed. For a survey on observed steering values, we refer to [SBES11, RDC+09].

The main ingredient for the experiment, which is schematically depicted in Fig. 3.3, is the source of squeezed light at 1550nm. The squeezing is generated by type I parametric down-conversion in a periodically poled potassium titanyl phosphate crystal (PPKTP). This crystal is coated and cut to form a half-monolithic cavity, which is driven at a pump frequency of 775nm and temperature controlled to achieve phase matching. The 775nm light is itself created in an up - conversion process inside another PPKTP crystal from a 1W driving laser at 1550nm. From this driving laser, a fraction is removed to form the local oscillators for the homodyne detection.

The variances of the squeezed and anti-squeezed quadrature that is achievable in this setup is defined by the properties of the squeezer and the initial pump power

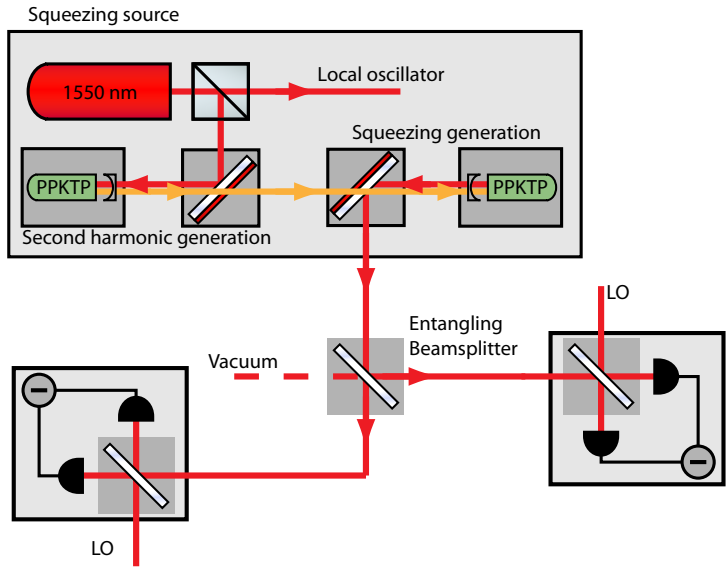

Figure 3.3.: Schematics of the squeezed light source and the homodyne detection. Red lines indicate the path of 1550nm light, orange lines indicate path of 775nm light.

(see e.g. [TYYF07] and references therein). We can empirically describe the functional connection as

$$\mathrm{Var}_{sq,asq}(P) = 1 \pm \eta\gamma \frac{4\sqrt{P/P_0}}{(1 \mp \sqrt{P/P_0})^2 + 4k(f)^2}, \tag{3.29}$$

where η is the detection efficiency, γ the escape efficiency of the squeezing cavity, P_0 is the threshold power and $k(f) = 2\pi f/\kappa$ the ratio between the Fourier frequency f and the cavity decay rate $\kappa = (T+L)c/l$, where T is the output coupler transmission, L the intra cavity loss, c the speed of light and l the cavity round trip length. In the given experiment, fixed parameters were $f = 5$MHz, $l = 79.8$mm, and the parameters that were determined via a fit of the measured data were $\eta\gamma = 0.91$, $P_0 = 445$mW and $T + L = 0.105$.

Results of the measurement are presented in Fig. 3.4. For different values of the pump power the amplitude and phase quadratures for Alice and Bob were measured, each for $5 \cdot 10^6$ times, then the conditional variances were calculated and the corresponding EPR value was determined. Error bars for the pump power were es-

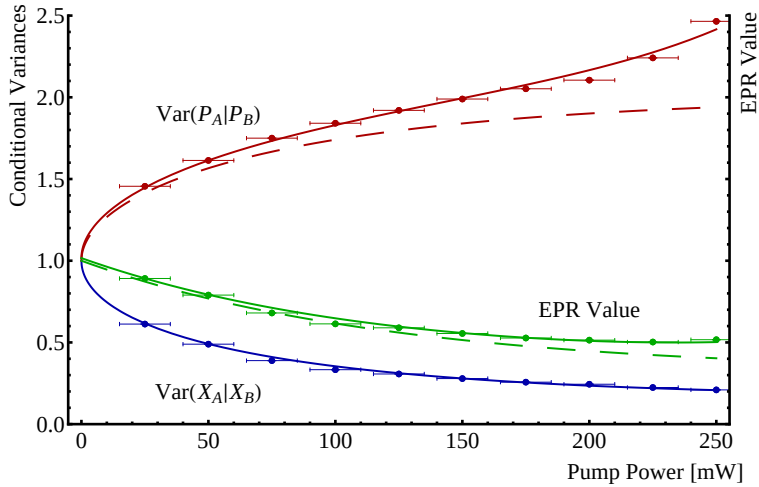

Figure 3.4.: Experimental results and theoretical model for the conditional variances of the X quadrature (blue) and P quadrature (red) and the EPR value (green). The solid lines represent the theoretical model with excess noise, the dashed lines the model without excess noise for comparison. For the X quadrature, the two models coincide.

timated from experimental considerations. For comparison, we have plotted the theoretical curves corresponding to equation (3.29), where we found a good agreement with the experimental findings for the amplitude quadrature (solid blue line), but a significant deviation in the phase quadrature (red dashed line). This difference was later identified as classical excess noise due to detector saturation. We have modeled this pump power dependent effect, by adding a noise of the form

$$EN(P) = \frac{\eta_{EN}}{(1-\sqrt{P/P_0})^2}, \tag{3.30}$$

where $\eta_{EN} = 0.016$ leads to the best fit.

One should note here, that other sources of noise are in principle also possible, where a prominent candidate would be phase noise [FHD+06]. We did, however, not observe significant signs of phase noise in the data, so this source of noise could be neglected (cf. [EHD+11a, 6.1])

The minimal value for the EPR parameter that was reached in this experiment was 0.502 ± 0.006 for a pump power of 225 mW. As mentioned in the beginning of this section, in later experiments lower values could be realized. In [EHD+11a] a

value of 0.31 was reached with a similar experimental setup for v-class entanglement. This could be achieved by significantly reducing the excess noise. To our knowledge, the lowest EPR value observed up to now was 0.04 in an experiment using two sources of squeezed light at 1064nm [SBES11].

3.2.3. One-way steering

From the definition of steering, one sees that steering is an asymmetric quantity, i.e., the roles of Alice and Bob in the bipartite case are not interchangeable. This means that there are cases in which models exist that are classical on Alice's side and quantum on Bob's side, but not vice versa. This is a different situation from the existence of a general classical model for both sides, i.e., the non-violation of all Bell inequalities, and also from the existence of a separable quantum model. Between these notions, there is again a strict hierarchy. The violation of at least one Bell inequality implies the steering effect for both directions, while the steering effect for one direction implies the non-separability of the state.

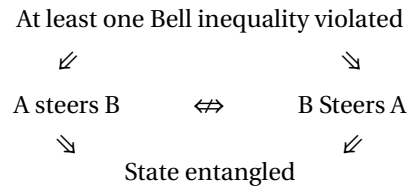

Figure 3.5.: Implications of directed steering.

We have depicted the logical implications in Fig. 3.5. The question, in which situation the converse implications holds, is still open. We know that none of the converse implications hold for qubits, and we will see that the same is also true in the Gaussian regime. What follows directly from Fig. 3.5 is, that the existence of one-way steering also implies that entanglement cannot automatically imply the violation of a Bell inequality, i.e., there have to exist entangled states that do not violate any Bell inequality.

The existence of a genuine one-way situation, i.e., a situation that is steering in one direction but not the other, was posed as an open question in [WJD07]. In [WJD$^+$08], steering with asymmetric strength was discussed for the first time. In [MFO10], a setup for the observation of one-way steering in the Gaussian regime was proposed, which is based on an intra-cavity nonlinear coupler and thus different from our approach. While for the general situation, no answer can be given yet, in the special case of the Gaussian regime such a situation can be experimentally demonstrated, which has recently been performed at the AEI in Hannover

[HES+12].

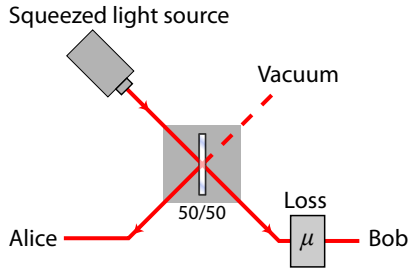

Figure 3.6.: Sketch of the setup for the demonstration of one-way steering.

The experimental setup is depicted in Fig.3.6. As the source of squeezed light at 1550nm we use again a type I parametric down conversion in a half-monolithic cavity. The entanglement is created by superimposing this light with a vacuum mode on a 50/50-beamsplitter. The two output beams are then sent to Alice and Bob, who perform homodyne detection. For details on the setup, compare the description in section 3.2.2. The asymmetry is then realized by adding variable loss to Bob's arm in the setup. The loss is modeled by sending the light through a half wave plate and a polarizing beam splitter.

The experimental results, together with a numerical simulation are depicted in Fig. 3.7. As criterion for the steering effect, the Reid-EPR value was calculated from the experimental data for both directions, i.e.

$$\mathrm{EPR}(A|B) = \mathrm{Var}\,(X_a|X_b)\cdot\mathrm{Var}\,(P_a|P_b) \quad \text{and} \quad \mathrm{EPR}(B|A) = \mathrm{Var}\,(X_b|X_a)\cdot\mathrm{Var}\,(P_b|P_a). \tag{3.31}$$

The advantage of using the conditional variances is, that no full tomography is required. As we have seen in section 3.2.1, for the correct choice of local basis, the Reid-EPR value will exactly match the minimal value that is obtained by evaluating the EPR value from the symplectic invariants

$$\mathrm{EPR}(A|B) = \frac{I_4}{I_1} \quad \text{and} \quad \mathrm{EPR}(B|A) = \frac{I_4}{I_2}. \tag{3.32}$$

For the numerical simulation we used a model with input squeezing and anti-squeezing as free parameters and the excess noise fixed to 1%. The best fit for the two graphs in Fig. 3.7 is then obtained for a squeezing of 10.2 dB and an anti-squeezing of 15.6 dB. The squeezing value of 10.2 dB was also directly confirmed from an independent measurement. To determine the statistical variation subsets

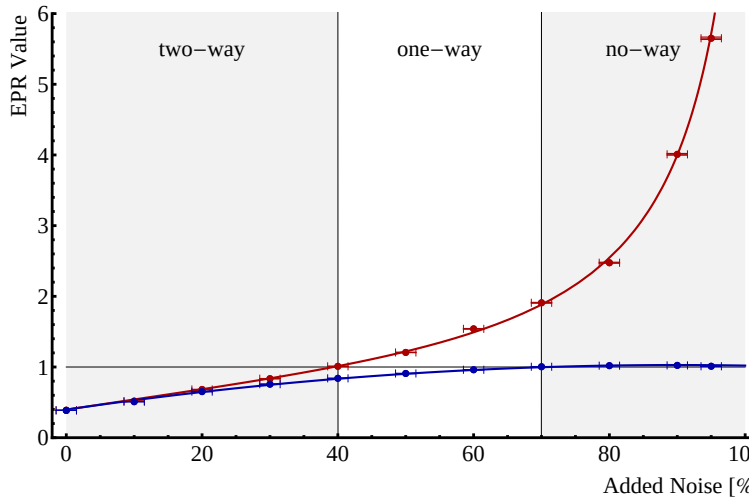

Figure 3.7.: Experimental results (dots) and theoretical model (lines) for the EPR values for different additional losses on Bob's side. Blue: EPR(A|B), Red: EPR(B|A). The shaded areas indicate the regions with two-way, one-way and no steering.

of length 10^6 were chosen for 10^4 times from the original sample of $5 \cdot 10^6$ measurement values. These deviations have been found to be relatively small (< 0.02) and hardly visible in the figure. The error bars on the vacuum contribution was estimated from the experimental situation.

What can be seen from Fig. 3.7 is, that the experimental and theoretical results match nicely. For a vacuum contribution below ca. 40%, the steering effect is visible in both directions, for a contribution above ca. 70%, no steering effect can be observed anymore. In the intermediate region one-way steering is visible in which the steering effect is present from Bob to Alice, but not vice versa.

3.2.4. Three partite situation

In the previous section we have seen that in the bipartite situation directed steering can be observed. If one considers a multi-party scenario, there arise a variety of possible situations in which a certain fraction of the parties might or might not be able to steer another fraction. As an example we will now discuss the three partite case between parties Alice, Bob and Charlie (A, B and C).

One first notes, that there are two different situations to be considered. The first are bipartite steering situations, in which one party steers a second party while the third party is ignored. These bipartite restrictions will also be called the one-to-one steering case. For instance one could ask, whether Alice is able to steer Bob's system, which we will call steering from A to B ($A \to B$). The second situation to consider is, when two parties are treated as one system, which we refer to as two-to-one or one-to-two steering. In this case, one could ask, whether Alice is able to steer Bob and Charlie ($A \to BC$ steering) or likewise if Bob and Charlie are able to steer Alice ($BC \to A$ steering). One should note here, that the term steering is even more misleading than in the bipartite case. An operational meaning has to be given first in terms of the probability distributions and the existence of a local model. If the system is, say, A to BC non-steering then there exists a classical model for Alice and a joint quantum model for Bob and Charlie producing the observed correlations. Likewise, the BC to A non-steering system has a joint classical model for Bob and Charlie and a quantum model for Alice. In this situation, we can extend theorem 3.2.1 to the multi partite case and get the extension of condition (3.13) as practical tool to check steering in the three partite case.

Definition 3.2.4. *A Gaussian state with covariance matrix γ is $A \to BC$ non-steering, if it holds that*

$$\gamma + i\Sigma_{BC} \geq 0, \tag{3.33}$$

where $\Sigma_{BC} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \Sigma & 0 \\ 0 & 0 & \Sigma \end{pmatrix}$ *is the symplectic form on the BC system.*

Likewise, the system is $BC \to A$ non-steering if it holds that

$$\gamma + i\Sigma_{A} \geq 0, \tag{3.34}$$

where $\Sigma_{A} = \begin{pmatrix} \Sigma & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ *is the symplectic form on A.*

One should note here, that the interpretation of the classical model treats two of the systems as one. In a $A \to BC$ non-steering situation, the measurement operators on the BC system, that give the right probability distribution, have no locality constraints on the joint BC system. In particular, there is no need that these are implementable with local operations and classical communications on the B and C system.

Even without considering the Gaussian case, we can extract some connections between the different types of steering. In fact, the one-to-two and two-to-one steering properties are largely determined by the one-to-one properties, as the following two theorems will show. The first theorem describes the dependence of the two-to-one situation of the one-to-one.

Lemma 3.2.5. *For any three partite steering situation we have*

$$C \to A \text{ steering} \Rightarrow BC \to A \text{ steering}, \tag{3.35}$$

Proof. We will prove the converse implication

$$BC \to A \text{ non-steering} \Rightarrow C \to A \text{ non-steering}. \tag{3.36}$$

By definition, the left hand side means that the joint three partite probability distribution $\mathbb{P}(a,b,c|A,B,C)$ can be written as

$$\mathbb{P}(a,b,c|A,B,C) = \int \mu(\mathrm{d}\lambda)\,\mathrm{tr}(\rho_A F_A(a)) \cdot f_{BC}(\lambda,b,c). \tag{3.37}$$

But then by ignoring the B system, we will get a valid response function for the B system alone, i.e., $f_B(\lambda,b) := \sum_c f_{BC}(\lambda,b,c)$ and

$$\mathbb{P}(a,b|A,B) = \int \mu(\mathrm{d}\lambda)\,\mathrm{tr}(\rho_A F_A(a)) \cdot f_B(\lambda,b), \tag{3.38}$$

which is the right hand side of 3.35. □

As we will see in the example below the converse is not true, i.e., there are states that are $BC \to A$ steering, but neither $C \to A$ nor $B \to A$. The following theorem shows the dependence of the one-to-two on the one-to-one case.

Lemma 3.2.6. *For any three partite steering situation it holds that*

$$A \to B \text{ steering} \Rightarrow A \to BC \text{ steering}. \tag{3.39}$$

Proof. Similar to the proof of lemma 3.2.5, one shows the converse implication, i.e.,

$$A \to BC \text{ non-steering} \Rightarrow A \to B \text{ non-steering}, \tag{3.40}$$

by showing that the model for the left hand side will give a model for the right hand side after ignoring the C system. □

The converse is again not true.

We finally note an implication between separability and two-to-one steering.

Lemma 3.2.7. *For a tripartite Gaussian state with covariance matrix γ_{ABC} under Gaussian measurements it holds that*

$$B - AC \text{ seperable and } C - AB \text{ seperable} \Rightarrow BC \to A \text{ non-steering}.$$

Proof. We start by restating the first condition on the left. The state is $B-AC$ separable, if it holds that

$$\Theta_B \gamma_{ABC} \Theta_B + i \begin{pmatrix} \Sigma & 0 & 0 \\ 0 & \Sigma & 0 \\ 0 & 0 & \Sigma \end{pmatrix} \geq 0,$$

where $\Theta_B = \mathbb{1}_2 \oplus \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \oplus \mathbb{1}_2$ implements the partial transpose on the B system. Multiplying from both sides with Θ_B we see, that this condition is equivalent to

$$\gamma_{ABC} + i \begin{pmatrix} \Sigma & 0 & 0 \\ 0 & \Sigma^T & 0 \\ 0 & 0 & \Sigma \end{pmatrix} \geq 0. \tag{3.41}$$

Likewise, using the second condition on the left the state is $C-AB$ separable, if

$$\gamma_{ABC} + i \begin{pmatrix} \Sigma & 0 & 0 \\ 0 & \Sigma & 0 \\ 0 & 0 & \Sigma^T \end{pmatrix} \geq 0. \tag{3.42}$$

Now we add equations 3.41 and 3.42:

$$\begin{aligned} \gamma_{ABC} + i \begin{pmatrix} \Sigma & 0 & 0 \\ 0 & \Sigma^T & 0 \\ 0 & 0 & \Sigma \end{pmatrix} + \gamma_{ABC} + i \begin{pmatrix} \Sigma & 0 & 0 \\ 0 & \Sigma & 0 \\ 0 & 0 & \Sigma^T \end{pmatrix} &\geq 0 \\ 2\gamma_{ABC} + i \begin{pmatrix} 2\Sigma & 0 & 0 \\ 0 & \Sigma^T + \Sigma & 0 \\ 0 & 0 & \Sigma^T + \Sigma \end{pmatrix} &\geq 0 \\ 2(\gamma_{ABC} + i \begin{pmatrix} \Sigma & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}) &\geq 0, \end{aligned}$$

which is, after dividing out the 2, the condition for $BC \to A$ non-steering. □

Example situation

As a model for three partite steering, we will discuss a setup that is similar to the one used in the one-way steering experiment in the previous section. We will again use a single source of squeezed light, which is superimposed with vacuum on a first beam splitter (BS1). One output is send to Alice, the second is superimposed with vacuum on a second beam splitter (BS2), whose two outputs are sent to Bob and Charlie. The situation is depicted in Figure 3.8.

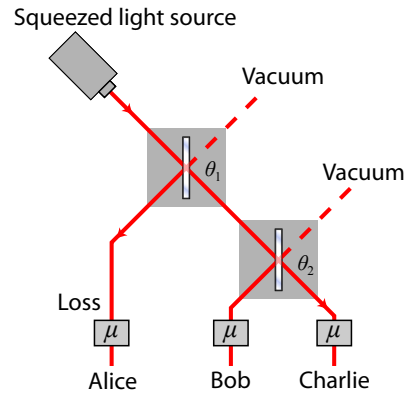

Figure 3.8.: Sketch of the setup for the demonstration of three-partite steering.

In general different sources of imperfections can be considered here. First, the state as produced by the squeezing source will not be a pure state in a real experiment. Furthermore, all optical paths will be subject to loss and possibly noise, as well as the measurement which will also introduce excess noise. To shorten the presentation, we will assume pure input states and apply symmetric loss. In our figures, we will fix the loses and chose the beam splitter angles θ_1 and θ_2 as parameters, which are linked to the transmittance t of a beam splitter via $t = \cos(\theta)^2$. We note that here the role of Bob and Charlie are interchangeable, i.e., the state on the Bob system with the second beam splitter set to $\theta_2 = \pi/r + x$ is the same as for Charlie with $\theta_2 = \pi/r - x$. A more formal treatment of noise sources will follow in section 4.5.1.

In Fig. 3.9 the results for the bipartite steering situations are depicted for a symmetric loss of 13%. We are only interested in whether steering is present, but not with which strength. This also means, that the input squeezing, which basically determines the squeezing contrast, is not so important in this case and will be fixed at 10 dB. We are thus varying the angles of the beam splitters, and see in which region which type of steering is present. In the six panels of Fig. 3.9, we have plotted the steering region for the six possible directions.

One notices that certain combinations of steering directions are not observed, namely that if the system is $A \to B$ steering it cannot be $C \to B$ steering at the same time. This also implies, that at the same time only three of the six possible steering directions can be present. In the left panel of Fig. 3.9 we have indicated how many of the individual one-to-one steering inequalities are violated. We note again the B to C symmetry.

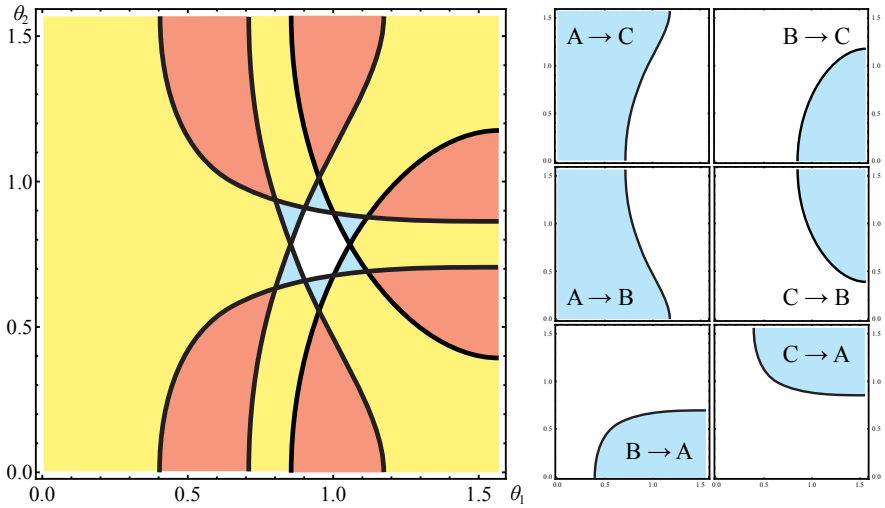

Figure 3.9.: Sketch of three partite steering regions. The six panels on the right show the regions in which the one-to-one steering is present. The left panel shows how many directions of steering can be observed at the same time. In red areas, three directions are present at the same time, in yellow regions two, in blue regions one and in the white region no one-to-one steering is present. The region does not cover the extreme angles 0 and π.

The number of one-to-one directions that are present at the same time is governed by the overall symmetric loss. The situation depicted in Fig. 3.9 is typical for a range of loss up to 25%. Between 25% and 33% there are no areas with three steering directions, but still six areas with two directions, while above 33% only three areas with two steering directions are left.

We remark, that in the figure the extremal values for the angles are not drawn, i.e., $\theta_{1,2} = (0, \pi/2)$. As we have noted above, the figures do not contain excess noise. This also means that steering is detectible even if the steering parameter is very close to 1. If one of the mirrors is tuned to full transmission or full reflection the corresponding steering inequalities cannot be violated any more, i.e., if the first mirror is reflective, no steering is observed, if it is transmitting, no violation from A or to A is observed, and the same reasoning holds for the second mirror and B or C respectively.

The situation for steering in the one-to-two setting is depicted in Fig. 3.10. Here, the behavior is again governed by the final loss. The figure shows the behavior up to

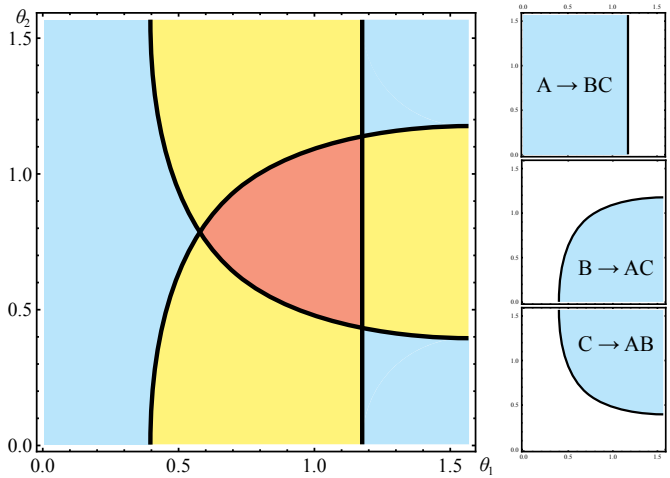

Figure 3.10.: Sketch of three partite one-to-two steering regions. The panels on the right show the regions separately, the panel on the left shows an overlay. The colors correspond to regions with one (blue), two (yellow) or three (red) simultaneous steering directions.

25% loss. Between 25% and 33%, the area with three steering directions vanishes, above 33% also the areas with two steering directions vanish and above 50% loss no steering is possible.

The situation for two-to-one steering is depicted in Fig. 3.11. It can be seen that this kind of steering is the easiest, in the sense that over a wide range of parameters, all three steering directions are present. The region with three steering directions will only vanish, if the loss is above 40%, and even up to 50% loss there remain three areas of two directions.

In summary, we have seen that with a single squeezed source and an appropriate adjustment of beam splitters, all interesting configurations of steering can be achieved in a tripartite setting.

3.3. Discussion and Outlook

Steering is one of the basic properties of quantum correlations and is equivalent to the question, whether a given probability distribution can be realized with a one-sided classical model. It can be used also in a situation in which the violation of a Bell inequality is not possible, e.g., in the Gaussian regime. Steering, in contrast to

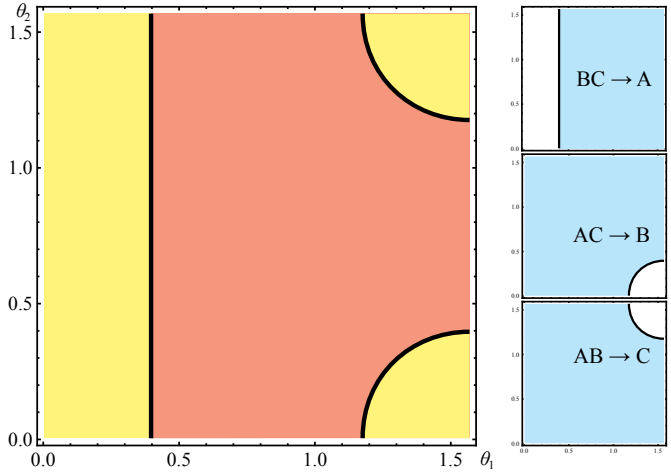

Figure 3.11.: Sketch of three-partite two-to-one steering regions. The panels on the right show the regions separately, the panel on the left shows an overlay. The colors correspond to regions with one (blue), two (yellow) or three (red) simultaneous steering directions.

entanglement or the violation of a Bell inequality, is a directed quantity and we have seen that a one-way steering situation for a bipartite setup can be experimentally realized. We have further shown how to extend this to the tripartite setting.

In contrast to the Gaussian regime, where the question when a state is steering can be decided by a condition on the covariance matrix, similar conditions are not known for finite dimensional systems. In [CHRW11] the concept of steering witnesses was introduced, in an analogous construction to Bell inequalities, but generally little is known about the structure of the non-steering set. It would be interesting to see, which configurations of steering can arise in a tripartite qubit situation. To our knowledge, directed steering has not been addressed explicitly for qubits. Another question that arises in connection with qubits are possible monogamy relations. It is known, that in the $(3,2,2)$-case there is a monogamy of the CHSH-inequality, namely if Alice and Bob can violate the CHSH inequality on some degrees of freedom, it cannot be violated on the same degrees of freedom between Alice and Chary or Bob and Charley. This is a specialty of the CHSH-inequality and does not hold for the $(3,3,2)$-case. It would be interesting to investigate, whether the same behavior is true for steering.

In the continuous variable case, a natural extension of the question would be, what steering situations arise, of one considers either a larger set of measurements

or non-Gaussian states. Here, the theoretical approach could be motivated by the study of different, experimentally realizable situations. On the other hand, if general measurements are considered it is not clear whether the set of states that permit the violation of a Bell inequality is strictly smaller than the steering set. It might be an instructive endeavor to construct a state that is not violating any Bell inequality but is steering for arbitrary measurements.

Finally, there is the question if there are general connections between steering and quantum communication. In [BCW+12] it wa shown that steering is necessary for one-sided device independent cryptography. The intuition behind this is straightforward: if a system is non-steering from Alice to Bob, then there is a classical model on Alice's side and when her devices are untrussed, Eve could have full information about her system.

4. Cryptography with Gaussian states

Overview and Contributions

This chapter describes a new cryptographic security proof and a modified protocol for entanglement based cryptography with continuous variable (CV) quantum states. The work was performed in cooperation with F. Furrer, V. Scholz and R.F. Werner from the quantum information theory group in Hannover and M. Berta, A. Leverrier and M. Tomamichel from the ETH Zürich. Our main contribution is the application of the entropic uncertainty relation to a CV-QKD protocol, the estimation of the max-entropy in this case and the numerical optimization of the system parameters in the simulation under realistic conditions. Results were presented in [FFB+12]. Estimations of the experimental parameters were done in collaboration with T. Eberle and V. Händchen from the group of R. Schnabel at the Albert Einstein Institute in Hannover.

4.1. Setting and assumptions

The goal of any cryptographical scheme is to allow some parties to perform a communication task, in our case, to communicate without being spied on by an eavesdropper. The power of a cryptographic scheme is measured on the one hand in the amount of information that can be transmitted in a given time and on the other hand on the assumptions made in the derivation. We start this chapter by first presenting our setup and the assumptions in a concise but non-technical way. The technical details will be presented in the respective sections below. The main reason for this is, that we find the presentation easier to follow, even if this requires some repetition.

We will be interested in cryptographic situation in which two parties, Alice and Bob, want to establish a key which is secure against an eavesdropper, called Eve. The main assumption made in the following is, that Alice and Bob are in full control over their laboratories. This means, that we can make a clear separation of the zones of influence of Alice, Bob and Eve. We will be interested in a entanglement based protocol, in which an entangled state is prepared and one part of this state is given to each of the two parties.

In many studies of entanglement based cryptography in the literature, this source is given to Eve, thus giving her full control over the state. As we will explain below, this is not easy in our situation, which is why we will place the source in Alice's lab. With this, the situation can be described as follows: Alice prepares in her lab a certain number of bipartite states and sends one half of each state to Bob. During the transmission, Eve is allowed to interact with the states in any way allowed by quantum mechanics. Upon arrival of the states at Bob's laboratory, she is not able to interact any more, only Bob is allowed to perform measurements. The procedure in which the states are prepared and measured are known beforehand to all parties and we assume, that they can be performed arbitrarily well. The main requirement here is, that the devices operate stationary and memoryless. Other imperfections will simply be attributed to Eve. For example, noise in the phase of the detectors will diminish the quality of the correlations an thus reduce the secret key rate, possibly overestimating the lost secrecy.

At the end of the chapter, we will make a comparison of the key rates obtained by our estimation with the key rates obtained under the assumption of collective Gaussian attacks,i.e., an eavesdropper that is, in addition to the restrictions above, confined to performing permutation invariant Gaussian attacks.

Let us further note, that we are interested in finite runs of the experiment. In this case, one has to be careful how to define the expectation for security. We will give the definition below, but observe here, that in any finite run of the protocol, there is also a finite probability for the eavesdropper to correctly guess the key, even if he has no interaction with the experiment, simply because the set of possible keys itself is finite. His success probability will decrease exponentially with the number of signals, but will remain strictly positive. In this sense, we can only hope to achieve a protocol, which is secure except some small probability. To determine this probability the protocol will have some security parameters that are chosen in accordance to the available experimental situation. Especially, they will be chosen in accordance with the total number of transmitted signals.

After this introduction, let us first go through the different steps of a key distribution protocol:

Step 0: Preliminaries Prior to the actual key distribution, two steps have to be performed: First, Alice and Bob have to make sure, that they are indeed who they claim to be. We will not discuss this authentication step this in the following, but list it here as an remark. In practical application one way to ensure this, is to assume that Alice and Bob have a pre-shared key, that is only used for authentication. For details on such schemes consult [Sti91, GN93]. Second, they agree on the parameters used in the experiment. This step was already mentioned above and ensures, that the two parties know about all details of the implementation and determine the appropriate security parameters according to the protocol.

Step 1: The quantum phase In this phase, all quantum signals are processed. It

is divided in the following steps:

1. Distribution: first a number of signals is given to Alice and Bob. In our specific protocol, the parties will loose half their signals to sifting, so we assume a number of $2N$ signals distributed.

2. Measurement: Alice and Bob measure the incoming signals according to the protocol, in our case in one of two quadratures. Via public communication they discard the measurement results, where the bases did not match and are left with strings of length N. We call these strings the raw key X_A and X_B and the state shared between Alice and Bob $\omega_{X_A X_B}$. We call the purification of this state onto Eve's system $\omega_{X_A X_B E}$.

3. Parameter estimation: they reveal their measurement results on a randomly chosen substring of length k. From this, they calculate the quality parameter and compare if this parameter matches their expectation. If this is the case, they continue with the protocol, otherwise, they abort.

The process of agreeing on the measurement bases and discarding the bits in which the bases did not match is also called sifting, the key after this step is referred to as the sifted key (see e.g. [SBPC$^+$09] for a survey). To keep the notation the the following shorter, we fix the number of bits after sifting and always assume that during the sifting process, exactly half of the signals are lost.

Step 2: The classical phase After the quantum phase has been completed and the protocol did not abort, Alice and Bob know, that the run of the protocol was within the expected range that they have agreed on beforehand. In particular, they know how much information could have been distributed to the eavesdropper. They now perform two classical post processing steps. First they perform error correction, in which they compare their strings and correct errors, that might have occurred during the communication. In the second step, called privacy amplification, they shorten the key while at the same time reduce the knowledge of the eavesdropper about the key. Both steps will be made more precise in the following. We call the strings after postprocessing S_A and S_B respectively, the length of the strings is l. The classical-quantum state here is called $\omega_{S_A S_B E}$. We call the average number of extractable secret bits per signal $r = l/N$ the secret key rate of the protocol. Note, that a rate depends on the specific parameters that are chosen in the process. Rates that are given in the limit if infinite number of transmitted signals are denoted r_∞.

Before giving the technical definitions, let us comment on the direction of classical communication. We have in the above description not specified, how the classical communication between Alice and Bob is exchanged, in particular whether Alice or Bob discloses parts of their information. In general, we could distinguish between two-way protocols, in which the communication is done in a multi round

dialogue between the parties, and a one-way scenario in which one party is essentially silent, apart from acceptance notifications. It is clear, that a two way communication is is principle stronger then the one-way one, but tight bounds for the performance of two-way protocols are in general not known, so we will also use one-way communication. In this case, there are two possible directions of communication. Either Alice is active, which is called direct reconciliation, or Bob is active, called reverse reconciliation (see e.g. [SBPC+09] and references therein). The two possibilities can give significantly different results, when the eavesdropper has different information about Alice's or Bob's key. In our case, however, the source of communication is placed into Alice's lab, which basically limits us to direct reconciliation. We will give all definitions with this situation in mind and comment at the end of the chapter on possibilities of applying reverse reconciliation.

4.2. Tools and definitions

4.2.1. Security definitions

After having described the goals and the setup in the previous chapter, we will now give the security definitions. As we have noted above, it is important to keep track of these values for any scheme working with a finite number of signals, as in this case the probability of an undetected error occurring in the protocol can never be exactly zero but only be made exponentially small in the number of signals sent. We will employ the definition of composable security and use the formalism developed in [Ren05, TLGR12, FAR11, BFS11].

Definition 4.2.1. *We call a bipartite state a classical-quantum state (cq-state), if it can be written in the following way:*

$$\omega_{cq} = \sum_{x \in X} p(x)|x\rangle\langle x| \otimes \omega_B^x, \tag{4.1}$$

where X is the alphabet on the A system and p a probability distribution, and ω_B^x states on the B system,.

In the protocol described above, Alice and Bob first perform their measurements, which results in the cq-state $\omega_{X_A X_B E}$. This state is then via classical post processing transformed into a cq-state on which the security is evaluated, and that is given as

$$\omega_{S_A S_B E} = \sum_{s_A s_B} p(s_A s_B)|s_A s_B\rangle\langle s_A s_B| \otimes \omega_E^{s_A s_B}. \tag{4.2}$$

We will now state the security definitions, where we use the formalism developed in [Ren05].

Definition 4.2.2. ***Robustness****: we call a protocol robust, if it does not abort in a situation in which no eavesdropper is present. We call the probability that an instance of the protocol does not abort P_{pass}.*

Correctness*: we call a protocol ϵ_c-correct, when*

$$Prob(s_a \neq s_b) \leq \epsilon_c. \tag{4.3}$$

Secrecy*: we call a protocol ϵ_s-secret, if*

$$P_{pass}|\omega_{S_A S_B E} - \tau_{AB} \otimes \sigma_E|_1 \leq \epsilon_s, \tag{4.4}$$

where $|\cdot|_1$ denotes the 1-norm, $\tau_{AB} = 1/d \sum_s |ss\rangle\langle ss|$ is a uniform mixture of correlated states and σ_E is an arbitrary state on Eve's system and P_{pass} denoted the probability that the protocol does not abort.

Security*: a protocol is ϵ- secure, if it is ϵ_c-correct and ϵ_s-secret with $\epsilon_c + \epsilon_s \leq \epsilon$.*

Let us note here, that with these definition, any instance of the protocol that is aborted is count as a success. In other words, a protocol with success probability 0 is perfectly secure. This also implies, that there is a natural tradeoff between the abort probability and the secrecy. If one considers the average rate, with which secret key can be generated from signals of a certain block length, the success probability can thus be treated like a free parameter that can be optimized to gain a higher secret key rate.

The main question of quantum key distribution is now, how long a secret key can be extracted from a given raw key. This question has been answered first in the context of finite dimensional systems in [Ren05] and later been generalized to infinite dimensional systems in [BFS11]. The main ingredient in the derivation are theorems about the efficiency of the classical post processing, i.e., the privacy amplification and the error correction, where the main technical quantities are the smooth min- and max-entropies. We will begin by introducing the smooth entropies in the next section, then give results on the classical post processing and finally give the key length formula that will be used later on.

4.2.2. Definition and properties of the smooth entropies

We will now give the definition of the smooth min- and max-entropies and recall their properties. For a more thorough treatment and proofs we refer to the literature [FAR11, BFS11]. An excellent reference for finite dimensional min- and max-entropies is [Tom12]. We note here, that log will in the following denote the binary logarithm, where ln denotes the natural logarithm.

Definition 4.2.3. *Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two separable Hilbert spaces. Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma \in \mathcal{S}(\mathcal{H}_B)$ be states. We define the conditional min-entropy of ρ_{AB} with respect to σ_B as*

$$H_{min}(\rho_{AB}|\sigma_B) = -\log\inf\{\lambda \in \mathbb{R} | \lambda \mathbb{1} \otimes \sigma_B \geq \rho_{AB}\}, \tag{4.5}$$

where we set $H_{min}(\rho_{AB}|\sigma_B) = -\infty$ if the condition cannot be fulfilled for any λ. We further define the conditional min-entropy with respect to a subsystem as

$$H_{min}(\rho_{AB}|B) = \sup_{\sigma_B \in \mathcal{S}(\mathcal{H}_B)} H_{min}(\rho_{AB}|\sigma_B). \tag{4.6}$$

The unconditional min-entropy can be obtained from this definition by considering a trivial system for B. Then, the unconditional min-entropy is just equal to $H_{\min}(\rho_A) = -\log||\rho_A||$ and thus given by the largest eigenvalue of ρ_A. We see, that this quantity is 0 for pure states and has a maximum of $\log d$ in a d-dimensional Hilbert space, obtained on the maximally mixed state. [1]

Definition 4.2.4. *We define the conditional max-entropy of the state ρ_{AB} with respect to the system B as*

$$H_{max}(\rho_{AB}|B) = -H_{min}(\rho_{AE}|E), \tag{4.7}$$

where ρ_{ABE} is a purification of ρ_{AB}.

This condition is also referred to as the duality condition; the max-entropy is called the dual of the min-entropy. Such duality relations also hold for other entropic quantities, e.g., the von Neumann entropy is self dual and the Rényi entropy of order α id dual to the Rényi entropy of order β for $1/\alpha + 1/\beta = 2$.

From the definition one can also determine the unconditional max-entropy, that can be given as $H_{\max}(\rho_A) = 2\log \mathrm{tr}\sqrt{\rho}_A$ and coincides with the Rényi entropy of order 1/2. Them minimal value is 0 for pure states and $\log d$ for maximally mixed states on a finite dimensional space of dimension d.

Definition 4.2.5. *We now define the epsilon smooth min-entropy:*

$$H^{\epsilon}_{min}(\rho_{AB}|B) = \sup_{\tilde{\rho}_{AB} \in \mathbb{B}^{\epsilon}(\rho_{AB})} H_{min}(\tilde{\rho}_{AB}|B), \tag{4.8}$$

where $\mathbb{B}^{\epsilon}(\rho_{AB})$ denotes the epsilon ball around ρ_{AB} measured in generalized fidelity.

Let us recall some of the operational interpretation of the smooth entropies:

Definition 4.2.6. *Consider the classical-quantum state $\rho_{XE} = \sum_x p(x)|x\rangle\langle x| \otimes \rho^x_E$ on the Alice/Eve System. We define the guessing probability as the probability that Eve correctly guesses Alice's state with an optimal strategy on her side. It is*

$$p guess(X|E) = \max_{\{E_x\}} \sum_i p_X(x) tr(E_x \rho^x_E), \tag{4.9}$$

where the maximum is taken over all POVMs on Eve's side.

[1] The unconditional min-entropy will not play a role in the following, so we will omit the term "conditional" and only talk about min-entropies.

Theorem 4.2.7. *[KRS09] It holds that*

$$pguess(X|E) = 2^{-H_{min}(X|E)}. \tag{4.10}$$

Proof. We give here the basic ideas of the proof in finite dimensions as presented in [KRS09], for an extension to infinite dimensional systems, we refer to [BFS11, Prop. 5.5]. We begin by reformulating the definition of the min-entropy 4.6. By including the parameter λ one gets an optimization over non-normalized states as

$$\begin{aligned} H_{\min}(\rho_{AE}|E) &= -\inf_{\sigma_E \leq 0, \mathrm{tr}\sigma_E = 1} \inf\{\lambda | \lambda \mathbb{1} \otimes \sigma_E \leq \rho_{AB}\} && (4.11)\\ &= -\inf_{\tilde{\rho}_E \geq 0} \{\mathrm{tr}\tilde{\rho}_E | \mathbb{1} \otimes \tilde{\rho}_E \geq \rho AB\} && (4.12)\\ &= -\inf_{\tilde{\rho}_E \geq 0, \mathbb{1}\otimes\tilde{\rho}_E \geq \rho_{AB}} \mathrm{tr}\tilde{\rho}_E. && (4.13) \end{aligned}$$

Now one observes that the last optimization is a semi-definite program. One now shows that the following duality relation holds:

$$\inf_{\tilde{\rho}_E \geq 0, \mathbb{1}\otimes\tilde{\rho}_E \geq \rho_{AB}} \mathrm{tr}\tilde{\rho}_E = \sup_{E_{AE} \geq 0, \mathrm{tr}_A(E_{AE}) = \mathbb{1}_E} \mathrm{tr}(\rho_{AE} E_{AE}). \tag{4.14}$$

Furthermore, if the state ρ_{AE} is classical on A, the optimization can be restricted to operators E_{AE} that are classical with respect to A. □

Definition 4.2.8. *We define the epsilon smooth max-entropy as*

$$H^{\epsilon}_{max}(\rho_{AB}|B) = \inf_{\tilde{\rho}_{AB} \in \mathbb{B}^{\epsilon}(\rho_{AB})} H_{max}(\tilde{\rho}_{AB}|B). \tag{4.15}$$

Then the following duality theorem holds:

Theorem 4.2.9.

$$H^{\epsilon}_{max}(\rho_{AB}|B) = -H^{\epsilon}_{min}(\rho_{AE}|E), \tag{4.16}$$

where ρ_{ABE} is a purification of ρ_{AB}.

The following theorem is known as the data processing inequality. It states, that the application of a local channel to the bipartite state will only increase the entropies. In its general form it is given as follows:

Theorem 4.2.10. *Let ω_{AB} be a bipartite quantum state, $T : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_{B'})$ a channel, then it holds that*

$$\begin{aligned} H^{\epsilon}_{min}(A|B)_{\omega} &\leq H^{\epsilon}_{min}(A|B')_{\mathbb{1}_A \otimes T(\omega)} && (4.17)\\ H^{\epsilon}_{max}(A|B)_{\omega} &\leq H^{\epsilon}_{max}(A|B')_{\mathbb{1}_A \otimes T(\omega)} && (4.18) \end{aligned}$$

This theorem was proved for finite dimensional systems in [TCR10] and extended to infinite dimensional system in [FAR11, Prop. 2] and [BFS11, Prop. 4.15].

The following corollary quantifies, that from the fact that two states are close in purified distance, one can also bound the distance of their epsilon-entropies.

Corollary 4.2.11. *Let $\omega, \tilde{\omega}$ be two quantum states with $\mathcal{P}(\omega, \tilde{\omega}) \leq \epsilon'$. Then it holds:*

$$H_{min}^{\epsilon+\epsilon'}(A|B)_{\tilde{\omega}} \geq H_{min}^{\epsilon}(A|B)_{\omega} \tag{4.19}$$

$$H_{max}^{\epsilon}(A|B)_{\omega} \geq H_{max}^{\epsilon+\epsilon'}(A|B)_{\tilde{\omega}} \tag{4.20}$$

Proof. The corollary follows directly from the definition. As the ϵ-ball around ω is completely contained in the $\epsilon+\epsilon'$-ball around $\tilde{\omega}$, the optimization will be evaluated over a strictly larger set for $\tilde{\omega}$, resulting in the given inequalities. □

An important property of the min- and max-entropies is their behavior in the i.i.d. limit. Here, both entropies asymptotically coincide with the von Neumann entropy. This behavior can be quantified using the asymptotic equipartition property (AEP).

Theorem 4.2.12. *Let $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a state with $H(A)_\rho < \infty$. Then for any $\epsilon > 0$ it follows that*

$$\frac{1}{n} H_{min}^{\epsilon}(A^n|B^n)\rho^{\otimes n} \geq H(A|B)_\rho - \frac{1}{\sqrt{n}} 2\log(\eta)\sqrt{\log\frac{2}{\epsilon^2}}, \tag{4.21}$$

and

$$\frac{1}{n} H_{max}^{\epsilon}(A^n|B^n)\rho^{\otimes n} \leq H(A|B)_\rho + \frac{1}{\sqrt{n}} 2\log(\eta)\sqrt{\log\frac{2}{\epsilon^2}}, \tag{4.22}$$

where $n \leq (8/5)\log(2/\epsilon^2)$ and $\eta = 2^{-\frac{1}{2}Hmin^{(A|B)_\rho)}} + 2^{\frac{1}{2}Hmax^{(A|B)_\rho)}} + 1$.

The proof of this theorem was given for finite dimensional systems in [TCR09] and extended to infinite dimensions in [FAR11, Prop. 8]. One should note here, that $H(A^n|B^n)_{\rho^{\otimes n}} = nH(A|B)_\rho$.

From this, one directly deduces that the following limits hold:

Corollary 4.2.13.

$$\lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_{min}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) = H(\rho_{AB}|B) = \lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_{max}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n). \tag{4.23}$$

4.2.3. Error correction

The first step in the classical post processing is the error correction, where we will describe a one-way error correction with Alice as sender and Bob as receiver, i.e., a direct reconciliation protocol. For a reverse reconciliation protocol, their roles are inverted.

The overall target of this step is for Alice and Bob to remove errors from their strings of bits, so that afterwards they hold two copies of the same string. Error correction is performed without paying any special attention to the fact that Eve might be listening in, so all the communication that is used here is given to Eve which will reduce the amount of secrecy hold by Alice and Bob. The task of error correction is thus to determine, how many bits Alice has to send to Bob, such that Bob is able to make his string equal to Alice's. In the i.i.d. setting, this problem has been answered for classical systems by the Slepian-Wolf theorem [SW71] and in the case of a quantum system by Devetak and Winter [DW03]. In these publications it was shown that in both cases, the asymptotically optimal achievable rate is given by the conditional entropy $H(X|B)$, where B is either quantum or classical. In the case of finite repetitions, the solution was given by Renes and Renner in [RR12] for finite dimensional systems on Bob's side and for infinite dimensional systems in [BFS11][2].

We start by assuming a classical-quantum state ω_{XB} between Alice and Bob. To explicitly model the error correction procedure, we add a system C for the classical communication, where we call the alphabet for the messages also C. Then the error correction code consists of an encoding operation $E : l^1(X) \to l^1(C)$ on Alice's side and a decoding operation $D : l^1(C) \otimes \mathcal{S}(\mathcal{H}_B) \to l^1(X)$. The number of bits transmitted from Alice to Bob is then given as $\log_2 |C|$. For any value of the classical message, we can describe the decoding operation as POVM $\{D_x^c\}_{x\in X}$. An error correction scheme is then defined by the collection (C, E, D).

Definition 4.2.14. *Let ω_{BX} be a classical-quantum state between Alice and Bob and (C, E, D) an error correction scheme. The error probability of the scheme for the given state is given as*

$$p_{error}(\omega_{XB}) = 1 - \sum_{i=1}^{X} \omega_B^x \left(D^{E(x)_x} \right). \tag{4.24}$$

The following theorem states states, how to bound this quantity by the smooth max-entropy. It was first proven in [RR12] and later extended in [BFS11, Thm 8.2].

Theorem 4.2.15. *Let ω_{BX} be a classical-quantum state between Alice and Bob. Then for any alphabet C with $|C| \leq |X| < \infty$ there exist an encoding and a decoding opera-*

[2] Note, that a preprint of the article [RR12] was available 2008.

tion such that the correction scheme (C,E,D) *satisfies*

$$p_{error} = \sqrt{\frac{1}{|C|} 2^{H_{max}(X|B)+3}}. \tag{4.25}$$

This theorem has a direct extension to epsilon entropies:

Theorem 4.2.16. *Let* ω_{BX} *be a classical-quantum state and* $\epsilon > 0$*. Then for any alphabet* C *with* $|C| \leq |X| < \infty$ *there exist an encoding and a decoding operation such that the correction scheme* (C,E,D) *satisfies*

$$p_{error} = \sqrt{\frac{1}{|C|} 2^{H^{\epsilon}_{max}(X|B)+3}} + 2\epsilon. \tag{4.26}$$

From this we can conclude, that for the situation in which Alice transmits a number of l_{EC} bits to Bob in order to perform the error correction there is an encoding and a decoding scheme that will perform the task except with a failure probability of at most p_{EC}, if

$$l_{EC} = \inf_{0 \leq \epsilon \leq p_{EC}/2} \lceil H^{\epsilon}_{\max}(X|B) + 2\log \frac{1}{p_{EC} - 2\epsilon} + 6 \rceil. \tag{4.27}$$

This can be seen by setting $|C| = 2^{l}_{EC}$ in (4.26). The number of bits is also referred to as the leakage of the protocol. It should be noted, that this bound is essentially optimal, as the following theorem shows:

Theorem 4.2.17. *Let* ω_{BX} *be a classical-quantum state and* $\epsilon > 0$ *and* (C,E,D) *an error correction code with* $p_{error} \leq \epsilon$*, then*

$$\log |c| \geq H^{\sqrt{2\epsilon}}_{max}(X|B). \tag{4.28}$$

Even though, the value from eq. (4.27) is theoretically achievable, the concrete implementation will additionally depend on the code used, and there is no general construction method known to actually achieve this. To account for this extra amount of classical communication that is needed in order to compensate for the non optimal protocol, one introduces a leakage parameter λ.

Definition 4.2.18. *We say that an error correction code has leakage parameter* $\lambda \geq 1$*, if it holds that in the limit of many repetitions*

$$l_{EC} \geq \lambda \cdot H(X|B). \tag{4.29}$$

It should be noted here again, that in the limit, the epsilon max-entropy coincides with the conditional von Neumann entropy.

For practical applications it is often more convenient not to work with the leakage parameter, but instead with a derived quantity, called the error correction efficiency (see e.g. [SBPC+09]). Here, the intuition is, that if the parties have classical strings X_A and X_B, the amount of equal bits that can be extracted in an optimal way is given by the mutual information between the strings $I(X_A|X_B)$. Then an error correction efficiency can be defined in the following way:

Definition 4.2.19. *Let (X_A, X_B) be bit strings and r_{EC} the number of extractable bits after error correction. Then an error correction code has efficiency β, with $0 \leq \beta \leq 1$, if it holds that*

$$r_{EC} \leq \beta I(X_A; X_B). \tag{4.30}$$

The two parameters λ and β cannot be converted into each other in a state independent way. We will see in section 4.2.6 below, that it holds that

$$\lambda = \frac{H(X_A) - \beta I(X_A; X_B)}{H(X_A|X_B)}. \tag{4.31}$$

In practice, any code will be used on a specific block length. That is, even if 10^9 sifted bits were available, they will usually not be handled at once, but divided into smaller blocks. This has basically computational reasons, i.e., the gain in efficiency on the code does not justify the overhead in computation. So, every practical code will only give his optimal performance for a limited set of parameters, which in principle should be accounted for when optimizing the QKD protocol. This investigation is, however, not part of the present thesis. In our protocol we will work in a regime with a fairly large alphabet and small Gaussian error, for which "of the shelf" codes are unfortunately not available. For the quantitative investigation we will assume, that a code with an error correction efficiency of $\beta = 0.95$ is available, which corresponds to a leakage parameter of $\lambda \approx 1.02$. This value corresponds to codes that have been used in a different parameter regime in [JKJL11].

4.2.4. Privacy amplification

The second step of the classical post processing is the privacy amplification. We will assume here, that Alice an Bob have already performed error correction, so they have identical strings at hand, which allows us to reduce the investigation to a two party situation, in which Alice holds a string X of length that she wants to decouple from Eve.

The intuition behind this is the following. Suppose Alice's sting has a length of n_X bits, and she knows that of these bits only a number of w bits are known to Eve. Then Alice applies a function f that maps her string to a smaller string K, possibly from a different alphabet, and reduces the number of bits to $n_K = n_X - w$. This function is called a hash function. The privacy amplification is successful, if

her new string K is uniformly distributed and the eavesdropper has no knowledge about it.

The techniques presented here have been applied in scenarios without side information in [BBR88, ILL89]. They were extended to classical side information in [BBCM95, RW05], to quantum side information on finite dimensional systems in [RK05, Ren05] and to infinite dimensional systems in [Fur09, FAR11, BFS11]. The main tool of the technique is the use of two universal hash functions.

Definition 4.2.20. *Let K, X be finite sets with $|K| \leq |X|$. Let $\{f\}$ be a family of functions $f : x \to K$ and $\mathbb{P}_f$ a probability distribution on this family. Then $(\{f\}, \mathbb{P}_f)$ is called a family of two universal $X \to K$ hash functions, if*

$$\mathbb{P}_f(f(x) - f(y)) \leq \frac{1}{|K|}. \tag{4.32}$$

The existence of hash functions was proven in [CW79, WC81]. They can be used to efficiently decouple a random variable from the environment by mapping it onto a new variable with reduced alphabet. How efficient this can be performed is determined by the following theorem:

Theorem 4.2.21. *Let ρ be a classical quantum state between Alice and Eve, K and X two finite sets with $|K| \leq |X|$ and $(\{f\}, \mathbb{P}_f)$ a family of two universal $X \to K$ hash functions. Denote the operator implementing the hash function on the Alice system by T_f. Then it holds that*

$$\mathbb{E}_f \left(||T_f(\rho) - \frac{1}{|K|} \rho_{\mathbb{1}} \otimes \rho_E|| \right) \leq \sqrt{|K| 2^{-H_{min}(A|E)_\rho}}, \tag{4.33}$$

where $\mathbb{E}_f$ denotes the expectation value over the hash function family, $\rho_{\mathbb{1}}$ is the maximally mixed state on $|K|$ symbols and ρ_E is the reduced state on the Eve system.

The proof has been given for finite dimensional systems in [Ren05, Cor. 5.6.1] and extended to infinite dimensional system in [BFS11, Thm. 7.4].

The theorem thus states, that by choosing the target alphabet K small enough, one can decouple the state arbitrarily well from the environment. For cryptographical application, however, one needs the extension of the theorem to epsilon entropies:

Theorem 4.2.22. *Under the same conditions as 4.2.21 for any $\epsilon \geq 0$ it holds that*

$$\mathbb{E}_f \left(||T_f(\rho) - \frac{1}{|K|} \rho_{\mathbb{1}} \otimes \rho_E|| \right) \leq \sqrt{|K| 2^{-H^\epsilon_{min}(A|E)_\rho}} + 2\epsilon. \tag{4.34}$$

From this, we can derive the estimation of the expected key length or a given secrecy parameter ϵ_s.

Corollary 4.2.23. *Let ρ be a classical quantum state between Alice and Eve, $\epsilon_s \geq 0$. Then using a family of hash functions, an ϵ_s-secret of length l can be extracted from ρ for all*

$$l \leq \sup_{0\leq\epsilon\leq\epsilon_s/2} \lfloor H^{\epsilon}_{min}(A|E)_{\omega} - 2\log\frac{1}{\epsilon_s - 2\epsilon}\rfloor. \tag{4.35}$$

4.2.5. Key length formula

We have now gathered the necessary tools to state the general key length formula, as first derived in [Ren05] for finite dimensional systems and generalized in [FAR11, BFS11] to infinite dimensional systems.

Theorem 4.2.24. *Given a classical-quantum state $\omega_{X_A X_B E}$ and classical communication from Alice to Bob, it is possible to extract an ϵ_s-secret and ϵ_c-correct key of length*

$$l = H^{\epsilon}_{min}(X_A|E) - l_{EC} - \log\frac{2}{\epsilon_1^2\epsilon_c}, \tag{4.36}$$

where $\epsilon \leq (\epsilon_s - \epsilon_1)/(2P_{pass})$. Here H^{ϵ}_{min} is the ϵ-min-entropy and l_{EC} is the leakage of the classical error correction code.

Proof. This theorem is a direct consequence of (4.2.21). From there we see that

$$\frac{1}{2}|\omega_{X_A E} - \tau_X \otimes \sigma_E| \leq \sqrt{|K|2^{-H^{\epsilon}_{\min}(X_A|E)}} + 2\epsilon. \tag{4.37}$$

To bound the right hand side by $\epsilon_s/\mathrm{P}_{\mathrm{pass}}$, one needs that

$$l \leq H^{\epsilon}_{\min}(X_A|E) - 2\log(\frac{\epsilon_s}{\mathrm{P}_{\mathrm{pass}}} - 2\epsilon), \tag{4.38}$$

from which the theorem follows with $\mathrm{P}_{\mathrm{pass}} \leq 1$. □

With this, the estimation of the length of extractable secret key is reduced to the calculation of the ϵ-min-entropy and the leakage term. The first term corresponds to the information that Eve has about Alice's key, the later to information revealed to Eve during error correction. We will now discuss properties of these terms.

We note that, as defined in the in 4.1, the symbol l will denote the length of the generated key after the transmission of N signals, where $r = l/N$ denotes the rate at which key is generated. It is understood, that the value of r will depend on N.

4.2.6. Asymptotic key rate

Before coming to the estimation in our case, we want to connect the key length formula with the known results for the asymptotically extractable key length.

Corollary 4.2.25. *For an infinite number of repetitions and perfect error correction, the key rate formula becomes:*

$$r = \lim_{n\to\infty}\lim_{\epsilon\to 0}\frac{1}{n}(H^{\epsilon}_{min}(X_A|E) - l_{EC} - \log(\frac{2}{\epsilon_s^2\epsilon_c})) = H(X_A|E) - H(X_B|E) \tag{4.39}$$

Proof. We use the asymptotic estimation 4.23 and the estimation of the leakage term 4.2.19. First observe, that in the limit, every state can be decomposed into tensor product states. For these states, the smooth entropies coincide asymptotically with the respective von Neumann entropy. With the estimation of the leakage term we arrive at:

$$\begin{aligned} r &= \lim_{n\to\infty}\lim_{\epsilon\to 0}\frac{1}{n}(H^{\epsilon}_{\min}(X_A|E) - l_{\mathrm{EC}} - \log(\frac{2}{\epsilon_s^2\epsilon_c})) && (4.40)\\ &= \lim_{n\to\infty}\lim_{\epsilon\to 0}\frac{1}{n}(H^{\epsilon}_{\min}(X_A|E) - H_{\max}(X_A|X_B) - \log(\frac{2}{\epsilon_s^2\epsilon_c})) && (4.41)\\ &= H(X_A|E) - H(X_A|X_B) && (4.42)\end{aligned}$$

□

From this, we can also recover a formulation, that is often found in the literature (see e.g. [SBPC+09]). By substituting the conditional entropies with the mutual information, we get

$$\begin{aligned} r &= H(X_A|E) - H(X_A|X_B) && (4.43)\\ &= H(X_A) - I(X_A;E) - H(X_A) + I(X_A;X_B) && (4.44)\\ &= I(X_A;X_B) - I(X_A;E), && (4.45)\end{aligned}$$

where we note, that the quantity $I(X_A:E)$ is evaluated for a strategy, which is maximally informative for Eve. This is known as the Holevo bound, so by setting

$$r = I(X_A;X_B) - \chi(X_A;E). \tag{4.46}$$

This formula is called the Devetak-Winter bound for the extractable secret key rate [DW05]. From this relation, we can now also clarify the correspondence between the two error correction parameters, mentioned in section 4.2.3. To account for the practical inefficiencies of error correction codes, one uses either the parameter $\beta \leq 1$ to bound the mutual information between Alice and Bob in 4.46, or the

parameter $\lambda \geq 1$ to estimate the leakage term in 4.44. If the key rates corresponding to the parameters should coincide, we see that

$$\beta I(X_A;X_B) - I(X_A;E) = H(X_A|E) - \lambda H(X_A|X_B), \tag{4.47}$$

which is true for

$$\lambda = \frac{H(X_A) - \beta I(X_A;X_B)}{H(X_A|X_B)}, \tag{4.48}$$

which is 4.31.

4.2.7. Entropic uncertainty relation

With the previous results, the calculation of the key rate amounts to the calculation of the smooth min-entropy and the leakage term. Unfortunately, the smooth min-entropy can only be calculated in certain cases (e.g. pure states). We will use an entropic uncertainty relation that allows us to estimate the min-entropy via the max-entropy. Entropic uncertainty relations have been studied in different forms for quite a while now [MU88]. The form we are using was put forward in [TR11] for finite dimensional systems and generalized to infinite dimensional systems in [BFS11].

Theorem 4.2.26. *Let ω_{ABC} be a state on a tripartite system, $\{E_A^x\}$ and $\{F_A^y\}$ POVMs an the A-system and $\epsilon \geq 0$. Then*

$$H_{min}^{\epsilon}(X|B)_\omega + H_{max}^{\epsilon}(Y|C)_\omega \geq -\log c, \tag{4.49}$$

where ω_{XB} and ω_{YC} are the classical-quantum states after measurement of E and F respectively and $c = \max_{x,y} \|(E_A^x)^{\frac{1}{2}} \cdot (F_A^y)^{\frac{1}{2}}\|^2$.

The proof for infinite dimensional systems can be found in section 6 of [BFS11].

We will first give a rough idea of how to apply the uncertainty relation in a cryptographic setting, the details will follow below. Suppose, the protocol runs with N measurements, then the outcome on Alice's side X_A will be acquired by measuring a tensor product of single operators chosen at random from E and F. Denote by X_A^c the complementary outcome distribution, i.e., the distribution corresponding to a measurement where on all places the E and F measurements are interchanged.

From the above definition it holds that:

$$H_{\min}^{\epsilon}(X_A|E)_\omega \geq -\log c - H_{\max}^{\epsilon}(Y_A|B)_\omega,$$

where we have changed the naming of the subsystem to correspond to Eve and Bob. Now we apply this to $Y = X^c$, so

$$H_{\min}^{\epsilon}(X_A|E)_\omega \geq -\log c - H_{\max}^{\epsilon}(X_A^c|B)_\omega.$$

Using that the measurement basis are chosen randomly for Alice and that the measurement operators are complementary, one shows that $X_A^c = X_A$ and

$$H_{\min}^{\epsilon}(X_A|E)_\omega \geq -\log c - H_{\max}^{\epsilon}(X_A|B)_\omega.$$

This holds for all choices of measurements on Bob's system, so after performing the actual measurement we arrive at

$$H_{\min}^{\epsilon}(X_A|E)_\omega \geq -\log c - H_{\max}^{\epsilon}(X_A|X_B)_\omega. \tag{4.50}$$

This expression will allow us to estimate the min-entropy between Alice and Eve with a max-entropy between Alice and Bob. We also see that the quality of this estimation will depend on the constant c.

4.3. Cryptographic Protocol

We will now describe the run of our protocol and the emergence of the different parameters, that can be adjusted. For practical purposes, we will assume, that the source of the quantum states is placed in Alice's lab and thus trusted. This is a technical assumption that will enable us to perform estimation 4.4.1 in a simple fashion. We will comment at the end of the chapter on possibilities of omitting this requirement. We will further only consider the quantum phase of the communication, the authentication and classical post processing will not be considered explicitly. We will also for convenience start with a highly symmetric situation, but will note this at the appropriate positions.

Step 0: Adjustment of parameters Before the actual quantum communication will take place, Alice and Bob have publicly agreed on the parameters of the protocol. In practice, this is an optimization procedure based on knowledge about the available source and the detectors. We will always assume that Alice and Bob have full knowledge about their devices, hence this optimization is possible. Alice and Bob will agree on a number of signals to sent and a security parameter. Then they optimize the working parameters of the protocol, e.g., the abort probability. Then they know that after a non-aborted run of the protocol, the extracted key will have the security desired. One should note, that this optimization might depend on further restrictions, like the availability of efficient error correction codes. Still, a non-optimal choice of parameters will only lead to a reduced key rate (possibly zero) but will not compromise the security.

Step 1: Sifting Alice will prepare a number of bipartite entangled states, of which she sends one half of each state to Bob. The measurement will be done in either the X or the P basis, and the outcome of each measurement will in principle be a real number, discretized with the precision of the measurement device. The first step is to discard all cases, in which their choice of basis did not match, which is done

via public communication. On average, they will end up with half the number of originally sent signals. The number of signals after sifting is denoted by N.

Step 2: Mapping to finite alphabet They will then map the outcomes onto the finite alphabet χ. This mapping comes with two free parameters, the cut-off distance α and the discretization parameter δ. Whenever in the experiment a result is observed with an absolute value larger then α, the protocol is aborted. This step is necessary for the application of the entropic uncertainty relation, as we will see below. Conditioned that the protocol does not abort, all values lie in the region $[-\alpha,\alpha]$, which we discretize into segments of length δ. For convenience we will choose δ such that the number of symbols in the alphabet $\chi = 2\alpha/\delta$ corresponds to a natural number. We will label the corresponding intervals of the real line as $I_- = (-\infty,-\alpha)$, $I_{x<0} = [x, x+\delta)$, $I_{x>0} = (x-\delta, x]$, $I_+ = (\alpha,\infty)$. For this choice, the number 0 is not part of the alphabet and $|\chi|$ is a even number. We denote the corresponding projectors by $X(I)$ and $P(I)$ respectively.

In principle, the choices of parameters could be different for Alice and Bob and also for X and P. We will see later that it is advantageous to choose the cut-off parameter as large as possible, to obtain a high key rate. If now, for instance, the loss on Bob's side was higher then on Alice's side, it would be a good idea to choose the α smaller for Bob then for Alice. For the moment, we will nevertheless only consider the symmetric situation in which Alice and Bob are interchangeable.

We will assume, that after this step, Alice and Bob end up with exactly N signals, that have all passed the cut-off criterion.

Step 3 - Parameter estimation test: From these N signals, they will then use a random subset the results of length k for the parameter estimation test. They will calculate the (generalized) Hamming distance of these outcomes, defined as

$$d_k(X,Y) = 1/k \sum_{i=1}^{k} |X_i - Y_i|. \tag{4.51}$$

If this observed parameter exceeds a preset value d_0, the protocol is aborted.

We note, that we do not take the statistical deviations due to the sifting process into account. In practice, Alice and Bob would agree in step 0 on an number of signals they want to distribute, which would then give a sifted key of roughly half this length. We on the other hand assumed that it is exactly half the length, while in principle the statistical variations should be included in the optimization of the protocol parameters.

4.4. Key length estimation

Let us start by giving a plain text description of how the estimation will proceed. We have seen in 4.2.24, that, given the security parameters, the only quantity to bound

in order to calculate the secret key rate is the conditional min-entropy of the state. The plan is then to use the entropic uncertainty relation to bound the min-entropy via the max-entropy, which is only possible if the state is basically localized on a finite region in space, otherwise the bound would become trivial. We have included an abort criterion to account for this, but we still need to bound the entropies of the actual state, with the state after restriction on the "non abort" space. After that, we will need to show that the parameter estimation test is indeed sufficient to bound the max-entropy of the state. Then we can use the bounds from privacy amplification to give the extractable key rate. In the process, different free parameters will emerge, making the proof a bit intricate.

We will now state the theorem and then start collecting the pieces needed for the proof. Note again, that in the following theorem the source of the states is assumed to be inside Alice's lab.

Theorem 4.4.1. *Let the security parameters ϵ_s and ϵ_c be given. Suppose that after the exchange of N signals, the protocol passes the parameter estimation test (with parameter d_0 on a subset of length k) and the cut off test (with parameters α, δ) and leaks l_{EC} bits of information during the error correction and the correctness test is passed. Then an ϵ_s-secret and ϵ_c-correct key can be extracted with length*

$$l = n\left[\log\frac{1}{c(\delta)} - \log\gamma(d_0+\mu)\right] - l_{EC} - \log\frac{1}{\epsilon_1^2\epsilon_c} + 2, \tag{4.52}$$

where $n = N-k$ is the number of signals after the parameter estimation test. Here $c(\delta)$ corresponds to the overlap of the measurement operators occurring in the entropic uncertainty relation and is given as

$$c(\delta) = \frac{\delta^2}{2\pi} S_0^{(1)}(1, \frac{\delta^2}{4})^2, \tag{4.53}$$

where $S_0^{(1)}$ is the first radial prolate spheroidal wave function of the first kind. The term $\log\gamma(d_0+\mu)$ corresponds to the estimation of the max-entropy and is given as

$$\gamma(t) = (t+\sqrt{1+t^2})\left(\frac{t}{\sqrt{1+t^2}-1}\right)^t, \tag{4.54}$$

and

$$\mu = |\chi|\sqrt{\frac{N(k+1)}{nk^2}\ln\frac{1}{\epsilon_s - \epsilon_1 - 2\sqrt{2g(p_\alpha, n)}}}, \tag{4.55}$$

and ϵ_1 is chosen such that $\epsilon_s - \epsilon_1 - 2\sqrt{2g(p_\alpha, n)} \geq 0$.

The remainder of this subsection will be devoted to the proof of this theorem. We will divide the proof into smaller sections and lemmata, that will give the result

when combined in the end. We note, that in [FFB+12] the variable parameter ϵ_1 was fixed to $\epsilon_s/2$.

Abort probability: We have noted that the protocol will abort, if a measurement outcome is observed whose absolute value exceeds the parameter α. We will again consider a symmetric situation, in which the systems Alice and Bob and the expectation values for the quadratures are equal. We further assume, that the source is located in Alice's lab and that the source produces i.i.d. states. Let us denote by p_α the probability that a value is observed, which does not lead to an abort, i.e., if we denote the state of a single run by ω, it holds that

$$\omega(X(I_{\{-|\chi|,|\chi|\}}) = \omega(P(I_{\{-|\chi|,|\chi|\}}) \geq p_\alpha. \tag{4.56}$$

Then, using the i.i.d. assumption, we see that the probability that at least one of N runs will abort is given by

$$g(p_\alpha, n) = 1 - p_\alpha^n. \tag{4.57}$$

We note here, that the value of α is a free parameter so the value of $g(p_\alpha, n)$ and can, in principle, be made arbitrarily small. We will see in the end that if one considered the final extractable key length, there is a tradeoff between the value of α and the estimation. This way, there will be an optimal α for a fixed value of n. To get a feeling for the orders of magnitude, we note that according to Thm. 4.4.1 the square root of the value of g should in the end be chosen small compared to the security parameter ϵ_s. We are at the moment only interested in a rough estimate of the orders of magnitude. According to definition, p_α is the probability, that a single signal does not exceed α, which should be chosen close to 1, so we consider $p_\alpha = 1 - 10^{-a}$ and $n = 10^b$. Then the value of g is given as $1-(1-10^{-a})^{10^b}$. We see that

$$\begin{aligned} g &= 1-(1-10^{-a})^{10^b} && (4.58)\\ &= 1-\exp(10^b \log(1-10^{-a})) && (4.59)\\ &\approx 1-\exp(-10^{b-a}), && (4.60) \end{aligned}$$

where we made a first order approximation in the last step, as 10^{-a} is small. We see, that this quantity will vanish only if $a > b$. Then, it further holds that

$$g \approx 10^{b-a}, \tag{4.61}$$

by approximating the exponential function. Since ϵ_s will be in the order of magnitude of 10^{-6} we see that $\sqrt{2g} < 10^{-6}$, which means that $b-a$ should roughly be 15. We will consider b up to 12 (realistic values should not exceed 10), so choosing $a \approx 30$ will suffice over the parameter range under consideration. For the state under consideration, this will lead to a value $\alpha \approx 35$.

Application of entropic uncertainty relation: As we have noted, we cannot apply the entropic uncertainty relation to the state directly, but first need to make the transition to the state conditioned on the event that the protocol does not abort after discretization. Then we will apply the uncertainty relation to the restricted state.

In the following, we keep explicit track of Alice's choices of measurement bases. This information will be revealed during the communication and is available to all parties. To do so, we introduce the random variable Z uniformly distributed over $\{0,1\}$. Then Alice's choice over a run of N measurements is given as z^N chosen from Z^N. Observe, that we use here that the random number generator is trusted to be i.i.d.. We associate the measurement basis X to $z=0$ and P to $z=1$. We further denote the complementary basis as $\overline{z}$. Then the pre-measurement state is given as

$$\omega_{0,ABEZ^N} = \sum_{z^N \in \{0,1\}^N} \omega_{ABE} \otimes \frac{1}{2^N} |z^N\rangle\langle z^N|. \tag{4.62}$$

The measurement operator corresponding to a single measurement site i will be denoted $P_i(z_i)$, with $P_i(0)=X$, $P_i(1)=P$. For a string of measurements z^N we likewise denoted $P(z^N)=\otimes_i P_i(z_i)$.

We now introduce two POVMs for Alice, the first one corresponding to measurements onto the finite alphabet χ and a second, where we extend the alphabet to cover all $\mathbb{Z}$, thus corresponding to an unrestricted measurement. We denote the elements of the first POVM by $x \in \chi$ by $\{X(x)\}$ and $\{P(x)\}$ respectively. From this we define the POVM including the explicit choice of measurement basis z^N as $\{P(x,z^N)\otimes|z^N\rangle\langle z^N|\}$ and the post-measurement state as $\omega_{X_A BEZ^N}$, where $X_A \in \chi^N$ is the classical outcome of the measurement. Similar we define the second POVM with $\tilde{x} \in \mathbb{Z}$ as $\{\tilde{P}(\tilde{x},z^N)\otimes|z^N\rangle\langle z^N|\}$ and the corresponding state as $\tilde{\omega}_{\tilde{X}_A BEZ^N}$, where now $\tilde{X}_A \in \mathbb{Z}^N$. With this definition, we are able to state the estimation:

Lemma 4.4.2. *With the notation above, the following two inequalities hold:*

$$H_{min}^{\epsilon+\epsilon'}(\tilde{X}_A|EZ^N)_{\tilde{\omega}} \geq H_{min}^{\epsilon}(X_A|EZ^N)_{\omega} \tag{4.63}$$

$$H_{max}^{\epsilon}(\tilde{X}_A|EZ^N)_{\tilde{\omega}} \geq H_{max}^{\epsilon+\epsilon'}(X_A|EZ^N)_{\omega}, \tag{4.64}$$

for $\epsilon' = \sqrt{\frac{2g(n,p_a)}{p_{pass}}}$.

Proof. To show the result, we need to bound the purified distance of the states ω and $\tilde{\omega}$. We denote by $\Lambda = \mathbb{Z}\backslash\chi$ the part of the natural numbers, which will result in an abort in the protocol and by $P^\Lambda(z^n) = \sum_{x\in\Lambda} P(x,z^n)$ the corresponding projector. We will apply this projector to the signals that have not been used during the parameter estimation. Then, by definition 4.57 and conditioning on the event that

the protocol did not abort, it holds that $\tilde{\omega}_{X_A^n}(P^\lambda)) = g(n,p_\alpha)/p_{pass}$. Let us denote the state conditioned on z^n as

$$\omega_{X_A BE}^{z^n} = \sum_{x^n \in \chi^n} |x^n\rangle\langle x^n| \otimes \omega_{BE}^{x^n,z^n}. \tag{4.65}$$

Then we can estimate the fidelity as

$$\mathcal{F}(\tilde{\omega}_{X_A BE}^{z^n}, \omega_{X_A BE}^{z^n})^{1/2} = \sum_{x^n \in \chi^n} \mathcal{F}(\tilde{\omega}_{BE}^{x^n,z^n}, \omega_{BE}^{x^n,z^n})^{1/2} \geq 1 - \frac{g(n,p_\alpha)}{p_{pass}}, \tag{4.66}$$

which is just a consequence from the fact that states are equal, except outside of χ. We further estimate $\mathcal{F}(\tilde{\omega}_{X_A BE}^{z^n}, \omega_{X_A BE}^{z^n}) = (1 - \frac{g(n,p_\alpha)}{p_{pass}})^2 \geq 1 - 2\frac{g(n,p_\alpha)}{p_{pass}}$, and see that for the purified distance

$$\mathcal{P}(\tilde{\omega}, \omega) \leq \sqrt{2\frac{g(n,p_\alpha)}{p_{pass}}}. \tag{4.67}$$

From this result, the lemma follows by application of the triangle inequality for the smooth entropies 4.2.11. □

In the last estimation we have acquired an "extra" classical register for the choice of basis. The next lemma tells us, that this register can for our estimation be neglected.

Lemma 4.4.3. *Let $\omega_{X_A BEZ^N}$ be given as defined above. It holds that*

$$H_{min}^\epsilon(X_A|EZ^N)_\omega \geq -n\log c(\delta) - H_{max}^\epsilon(X_A|BZ^N)_\omega \geq -n\log c(\delta) - H_{max}^\epsilon(X_A|X_B)_\omega \tag{4.68}$$

Proof. The first inequality is a direct extension on the proof of corollary 7.6 in [Tom12]. The idea is similar to the consideration following theorem (4.2.26). The second inequality is a consequence of the data processing inequality (4.2.10). □

Estimation of the max-entropy: In the last section we have seen, how to reduce the measured quantum state to the state restricted to a finite outcome set, and how to apply the entropic uncertainty relation to transfer a min-entropy estimation into a max-entropy estimation. In this section we show, how to give an upper bound for the max-entropy in terms of the observed Hamming distance of outcomes.

Theorem 4.4.4. *Let X, Y denote two strings of length n from an alphabet χ. Denote by $d_k(X,Y) = 1/k\sum_{i=1}^k |X_i - Y_i|$ the generalized Hamming distance. Let $d_{PE} = d_k(X_{PE}, Y_{PE})$ denote the observed distance during parameter estimation of a random subset of length k. Then the following holds:*

$$Prob\big(d(X,Y) \geq d(X_{PE}, Y_{PE}) + \mu\big) \leq \epsilon, \tag{4.69}$$

for

$$\mu = |\chi| \sqrt{\frac{N(k+1)}{nk^2} \log \frac{1}{\sqrt{P_{pass}}\epsilon}}. \tag{4.70}$$

Suppose, $d(X_{PE}, Y_{PE}) \leq d_0$ *then*

$$H^{\epsilon}_{max}(X|Y) \leq n \log \gamma(d_0 + \mu), \tag{4.71}$$

with

$$\gamma(t) = (t + \sqrt{1+t^2}) \left(\frac{t}{\sqrt{1+t^2}-1} \right)^t. \tag{4.72}$$

The proof will be divided into two parts: First we proof the estimation if no statistical error are considered, i.e., in the case of infinite repetition, then we will use sampling theory to estimate the typical deviation for a finite sample.

Lemma 4.4.5. *Let* χ *be a finite alphabet,* $\mathbb{P}(x,y)$ *a probability distribution over strings of length* n *on* $\chi^n \times \chi^n$*. For any* $d_0 > 0, \epsilon > 0$ *with* $Prob_{\mathbb{P}}(d(x,y) \geq d_0) \leq \epsilon^2$*,*

$$H^{\epsilon}_{max}(X|Y)_{\mathbb{P}} \leq n \log \gamma(d_0), \tag{4.73}$$

with $\gamma(x) = (t + \sqrt{1+t^2}) \left(\frac{t}{\sqrt{1+t^2}-1} \right)^t$.

Proof. From the definition 4.16 we know, that the smooth entropy is taken over distributions with an ϵ distance. Define the following distribution:

$$\mathbb{Q}(X,Y) = \begin{cases} \frac{\mathbb{P}(x,y)}{\text{Prob}_{\mathbb{P}}[d(x,y) \leq d_0]}, & \text{if } d(x,y) \leq d_0 \\ 0, & \text{else} \end{cases}. \tag{4.74}$$

We denote by $\mathcal{F}(\rho,\sigma)$ the fidelity and $\mathcal{P}(\rho,\sigma) = \sqrt{1-\mathcal{F}(\rho,\sigma)}$ the purified distance. Then $\mathcal{F}(\mathbb{P},\mathbb{Q}) = \text{Prob}_{\mathbb{P}}[d(X,Y) \leq d_0]$ and $\mathcal{P}(\mathbb{P},\mathbb{Q}) = \sqrt{\text{Prob}_{\mathbb{P}}[d(X,Y) \geq d_0]} \leq \epsilon$.

One should note here, that the distributions X and Y are purely classical objects, so we can use estimations for the classical max-entropy. We use, that the max-entropy can be bounded by the Rényi-0 entropy (see e.g. [Tom12] and appendix (A.3) for a definition and [TLGR12] for a similar estimation),

$$H^{\epsilon}_{\max}(X,Y)_{\mathbb{P}} \leq H_{\max}(X,Y)_{\mathbb{Q}} \leq H_0(X,Y)_{\mathbb{Q}}, \tag{4.75}$$

with

$$H_0(X,Y)_{\mathbb{Q}} = \max_y \log |\{x \in \chi^n; \mathbb{Q}(x,y) \neq 0\}|. \tag{4.76}$$

In our case this is

$$H_0(X,Y)_{\mathbb{Q}} \leq \log|\{x\in\chi^n; \frac{1}{n}\sum_{i=1}^{n}|x_i|\leq d_0\}| \tag{4.77}$$

$$\leq \log|\{x\in\mathbb{N}^n; \frac{1}{n}\sum_{i=1}^{n}|x_i|\leq d_0\}| \tag{4.78}$$

For any $\lambda>0$ it holds:

$$|\{x\in\mathbb{N}^n; \frac{1}{n}\sum_{i=1}^{n}|x_i|\leq d_0\}| \leq \sum_{x\in\mathbb{N}^n,\sum_{i=1}^{n}|x_i|\leq nd_0} 1 \tag{4.79}$$

$$\leq \sum_{x\in\mathbb{N}^n,\sum_{i=1}^{n}|x_i|\leq nd_0} \exp(-\lambda(nd_0-\sum_{i=1}^{n}|x_i|)) \tag{4.80}$$

$$\leq \sum_{x\in\mathbb{N}^n} \exp(-\lambda(nd_0-\sum_{i=1}^{n}|x_i|)) \tag{4.81}$$

$$= \exp(\lambda nd_0)\sum_{x\in\mathbb{N}^n}\exp(-\lambda\sum_{i=1}^{n}|x_i|)) \tag{4.82}$$

$$= \exp(\lambda nd_0)\prod_{i=1}^{n}\sum_{x_i\in\mathbb{N}}\exp(-\lambda|x_i|)) \tag{4.83}$$

$$= e^{\lambda nd_0}\left(\sum_{x\in\mathbb{N}}\exp(-\lambda|x|)\right)^n \tag{4.84}$$

$$= e^{\lambda nd_0}\left(\frac{1+e^{-\lambda}}{1-e^{-\lambda}}\right)^n, \tag{4.85}$$

where the last inequality is due to the geometric series. As this holds for any $\lambda\geq 0$, we can determine the minimum with respect to λ, which is attained at $\lambda_m=\log(1+\sqrt{\frac{1+\lambda^2}{d}})$. Putting this into the last equation gives the result. □

The next step to proof is to invoke the finite statistics from parameter estimation. Denote again X_{PE}, Y_{PE} the strings obtained from parameter estimation of length k, we have to estimate the probability that $d(X,Y)\leq d(X_{PE},Y_{PE})$ in the case that the protocol does not aboard,i.e., none of the observed measurement values exceeds α. Denote by $\mathrm{P}_{\mathrm{pass}}$ the probability, that the protocol does not aboard. Then by Bayes' theorem it follows that

$$\mathrm{Prob}[d(X,Y)\leq d(X_{PE},Y_{PE})+\mu|\text{“pass”}]\leq\frac{1}{\mathrm{P}_{\mathrm{pass}}}\mathrm{Prob}[d(X,Y)\leq d(X_{PE},Y_{PE})+\mu]. \tag{4.86}$$

The bound on $d(X,Y) \leq d(X_{PE}, Y_{PE})$ is obtained using standard methods from sampling theory [Ser74]. We have a sample of length N that is divided into the parameter estimation part of length k and the raw key part of length n, where $N = k+n$. We call the corresponding distances d_{tot} on the whole string, $d_{PE} = d(X_{PE}, Y_{PE})$ on the parameter estimation part and $d_{key} = d(X,Y)$ on the raw key part. We have that

$$N d_{tot} = k d_{PE} + n d_{key}. \tag{4.87}$$

We use the bound from [Ser74] to obtain $\forall \mu > 0$

$$\text{Prob}[d_{key} \geq a + \tilde{\mu} | d_{tot} = a] \leq e^{-2n\tilde{\mu}^2 \frac{N}{|\chi|^2(k+1)}}, \tag{4.88}$$

where $\chi = \lceil 2\frac{\alpha}{\delta} \rceil$ denotes the alphabet length and we have used, that two measurement values may only differ by $|\chi|$. From 4.87 it follows, that $d_{key} \geq d_{PE} + \mu \longleftrightarrow d_{key} \geq d_{tot} + \frac{k}{N}\mu$, so

$$\text{Prob}[d_{key} \geq d_{PE} + \mu] = \text{Prob}[d_{key} \geq d_{tot} + \frac{k}{N}\mu] \tag{4.89}$$

$$= \int_{a \geq 0} \text{Prob}[d_{tot} = a] \cdot \text{Prob}[d_{key} \leq a + \frac{k}{N}\mu | d_{tot} = a] da \tag{4.90}$$

$$\leq e^{-2n\mu^2 \frac{nk^2}{|\chi|^2 N(k+1)}}. \tag{4.91}$$

Now we combine the results. To show that $\text{Prob}[d_{key} \leq d_{PE} + \mu | \text{“}pass\text{”}] \leq \epsilon^2$ it suffices to show $\text{Prob}[d_{key} \leq d_{PE} + \mu] \leq \text{P}_{\text{pass}} \epsilon^2$. From this we get the estimation

$$\text{Prob}[d_{key} \leq d_{PE} + \mu] \leq e^{-2n\mu^2 \frac{nk^2}{|\chi|^2 N(k+1)}} \leq \text{P}_{\text{pass}} \epsilon^2, \tag{4.92}$$

which is true for

$$\mu = |\chi| \sqrt{\frac{N(k+1)}{nk^2} \log \frac{1}{\sqrt{\text{P}_{\text{pass}}} \epsilon}}, \tag{4.93}$$

which completes this part of the proof.

Now we have all the tools and estimations to proof Thm. 4.4.1.

Proof of Theorem 4.4.1. We denote by ω the state conditioned that the test was passed, by $\tilde{\omega}$ the unconditioned state and by $\epsilon' = \sqrt{2g(p_a, n)}$ the correction due to the restriction on the test. Denote the classical information revealed during sifting by Z.

Then we estimate

$$
\begin{aligned}
H_{\min}^{\epsilon}(X_A|EZ)_{\omega} &\overset{(4.63)}{\geq} H_{\min}^{\epsilon-\epsilon'}(X_A|EZ)_{\tilde{\omega}} && (4.94)\\
&\overset{(4.68)}{\geq} -n\log c - H_{\max}^{\epsilon-\epsilon'}(X_A|BZ)_{\tilde{\omega}} && (4.95)\\
&\overset{(4.64)}{\geq} -n\log c - H_{\max}^{\epsilon-2\epsilon'}(X_A|BZ)_{\omega} && (4.96)\\
&\overset{\text{dp}}{\geq} -n\log c - H_{\max}^{\epsilon-2\epsilon'}(X_A|X_B)_{\omega} && (4.97)\\
&\overset{(4.71)}{\geq} -n\log c - n\log\gamma(d_0+\mu(\epsilon-2\epsilon')). && (4.98)
\end{aligned}
$$

The inequality labeled dp is the data processing inequality 4.2.10. The theorem follows, if we use the key length formula (4.2.24) with ϵ_s replaced by $\epsilon_s - 2\sqrt{2g(p_\alpha, n)}$. □

4.5. Results and Discussion

In the last sections, we have derived the bounds needed to estimate the security of the cryptographic protocol. In this section we will estimate the expected key rates and compare to bounds from collective and asymptotic estimations.

4.5.1. Key rates against coherent attacks

We will now use the techniques derived above to calculate key rates that correspond to an achievable experiment. More precisely, we will use the parameters that have been realized in an experiment at the AEI in Hannover as basis for a numerical simulation of the experiment and the resulting key rate.

The main ingredient of the experiment is a source of two-mode squeezed light located in Alice's laboratory. This source will be built by two sources for single-mode squeezed vacuum states, whose light is superimposed on a 50/50 beam splitter, also referred to as the entangling beam splitter. From this, one output is sent to Alice's detector and one output is sent to Bob. For a basic description of such a source c.f. 3.2.2.

The source is characterized, by the squeezing (λ_{sq}) and anti-squeezing (λ_{asq}) values. We will use a decibel scale, such that the covariance matrix of a single squeezer before the entangling beam splitter is given as

$$
\gamma = \begin{pmatrix} 10^{-\lambda_{sq}/10} & 0 \\ 0 & 10^{\lambda_{asq}/10} \end{pmatrix}. \tag{4.99}
$$

It is always assumed, that the phases are calibrated in a way that the off-diagonal elements are zero. For a pure Gaußian state, the squeezing and anti-squeezing

parameters would coincide. We will however not assume, that the initial state is pure. We further assume the entangling beam splitter to be perfect and model two sources of loss for the channel: loss and excess noise.

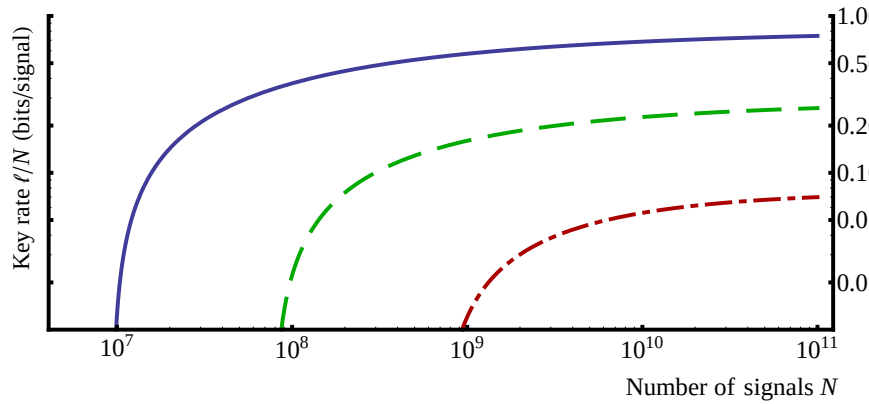

Figure 4.1.: Extractable key rate against number of sent signals for different values of loss: 0% (blue solid line), 4% (green dashed line) and 6% (red dot-dashed line). Input squeezing was 11 dB and anti-squeezing 16 dB. The excess noise was set to 1% and the security parameters to $\epsilon_s = \epsilon_c = 10^{-6}$ and the error correction efficiency $\beta = 95\%$.

Damping is an effect that is present in any optical transmission. Our setup employs squeezed light at 1550nm, which is transmitted through a low noise standard telecom fibre. The action of this channel is described as

$$\gamma \to (1-\mu)\gamma + \mu\gamma_{vac}, \tag{4.100}$$

where $\gamma_{vac} = \mathbb{1}$ is the covariance matrix of the vacuum state and μ is the damping factor. For 1550nm light, one expects a damping of 0.2 dB/km. This parameter will be varied later to account for different length of wires.

The second source of noise we consider is excess noise, which comes mainly from the classical data acquisition. Excess noise is modeled as white noise that is added to the channel, so via the mapping

$$\gamma \to \gamma + \nu\gamma_{vac}. \tag{4.101}$$

In our setup the technical noise is expected to be 20 dB below the signal, which corresponds to an excess noise of 0.01.

In figure 4.1, we have plotted the extractable key rate for different values of loss against the number of sent signals. We note, that we calculate key rates always in

bits, so more then one bit can be transmitted per run. As input states, we used always squeezing of 11 dB and anti-squeezing of 16 dB. The security parameters were set to $\epsilon_s = \epsilon_c = 10^{-6}$ and the error correction efficiency to $\beta = 95\%$. For this setting we see, that the minimal number of signals that have to be transmitted in order to get a positive key rate is $\approx 10^7$. If the excess noise is fixed to 1%, the limit for tolerable noise is 7%, which is reachable only if the number of signals approaches 10^{12}.

4.5.2. Asmyptotics of max-entropy estimation

The estimation of the key length formula 4.2.24 depends on the estimation of the min-entropy via the uncertainty relation and the max-entropy and the estimation of the max-entropy with 4.4. In order to evaluate our estimation for the max-entropy, we will now estimate the asymptotic behavior, as we know, that the max-entropy will converge to the von Neumann entropy in the limit on large number of repetitions N. We are also interested in the limit of $\delta \to 0$, which means that the resolution of the raw key will become arbitrary fine. This limit needs to be made cautious, as the definitions given in Chapter 4.2.2 have only been made with respect to a system on the Alice system with an arbitrary but fixed number of outcomes, not with continuous outcomes. This can be done but will not be discussed here.

For the analytical part we stick to an idealized situation to keep the derivation and notation simple. We start by considering an two-mode squeezed state ρ, defined by its covariance matrix Γ. We assume, that all losses are covered by the initial preparation and that the two generating squeezers are identical. Then the covariance matrix is given by the initial squeezing and anti-squeezing values.

In this case, the joint measurement of amplitude and phase on both sides has the same classical statistics.,i.e., $\Gamma_X = \Gamma_P$. Suppose (for sake of completeness), that the X quadrature is chosen with probability p_x, then it follows that

$$d(X|Y)_\Gamma = p_X d(X|Y)_{\Gamma_X} + (1-p_X) d(X|Y)_{\Gamma_Y} = d(X|Y)_{\Gamma_X}. \tag{4.102}$$

In our case, the distance has to be evaluated on the alphabet χ, so we have

$$d(X|Y)_{\Gamma_X} = \sum_{i=-|\chi|/2}^{|\chi|/2} \sum_{j=-|\chi|/2}^{|\chi|/2} |i-j| \int_{\square_{ij}} \mathrm{d}\xi W_{\Gamma_X}(\xi), \tag{4.103}$$

where the symbol $\square_{ij}$ indicates integration over the plaquette at position ij. For small δ, this sum can be replaced by the integral

$$d(X|Y)_{\Gamma_X} \approx \frac{1}{\delta} \int d\xi |\xi_1 - \xi_2| W_{\Gamma_X}(\xi) := d_a \tag{4.104}$$

This quantity however can be treated analytically. It holds that

$$d_a = 2\sqrt{\frac{\Gamma_{11}-\Gamma_{12}}{\pi}}\,\mathrm{Erf}[\frac{\alpha}{\sqrt{\Gamma_{11}-\Gamma_{12}}}] - \mathcal{O}(\exp[-\frac{\alpha^2}{2\Gamma_{11}}]). \tag{4.105}$$

Where Erf is the error function and $\Gamma = \Gamma_X$. We have collected all terms that vanish with α large enough. In this limit, the error function is one, and by plugging in the entries of the covariance matrix we arrive at

$$d_{ap} = 2\sqrt{\frac{\gamma_{11}-\gamma_{12}}{\pi}} = \frac{2}{\sqrt{\pi}}\sqrt{1}0^{-sq/10}. \tag{4.106}$$

If we now go back to the discrete version, the distance has to be scaled in units of δ, so $d_\delta = d_{ap}/\delta$. This approximation is good for small values of δ. In the limit $\delta \to 0$, for any fixed set of other parameters, the d_δ will become arbitrary large. We will next determine the behavior of γ. In the limit $x \to \infty$ it holds that

$$\log\gamma(x) \to \log(2ex), \tag{4.107}$$

where e is the Euler constant.

To see this, observe that $\lim_{x\to\infty}\left(x/(\sqrt{x^2+1}-1)\right)^x = e$.

Combining these results, we arrive at the asymptotic behavior

$$\gamma(d_{\delta\to 0}) = \log(\frac{4e}{\sqrt{\pi}}\sqrt{10^{-sq/10}})) - \log(\delta). \tag{4.108}$$

This results holds for an i.i.d. Gaussian state for α large enough, $N \to \infty$, $\delta \to 0$. In the same limit, we know, that the max-entropy converges to the conditional von Neumann entropy, which in this case is just the Shannon entropy of the classical distribution of the measurement results. So we can compare the quality of our estimation of the max-entropy in this asymptotic sense:

We start from 4.73

$$\frac{1}{N}H_{\max}(X|Y) \leq \log\gamma(d_0). \tag{4.109}$$

The left hand side will give in the limit the discrete version of von Neumann entropy

$$\frac{1}{N}H_{\max}(X|Y) \to H(X|Y)_\delta = \frac{1}{2}\log\left[\frac{4\pi e}{\delta^2}10^{-\frac{sq}{10}}\left(\frac{10^{\frac{asq}{10}}}{10^{\frac{asq}{10}}+10^{-\frac{sq}{10}}}\right)\right]. \tag{4.110}$$

We se that the term in the round brackets is approximately 1 if squeezing and anti-squeezing are high enough (say >10). For high enough squeezing in that sense we have

$$H(X|B) \simeq \log\left[\frac{2\sqrt{\pi e}}{\delta}\sqrt{10^{-\frac{sq}{10}}}\right] \leq \log\left[\frac{4e}{\delta\sqrt{\pi}}\sqrt{10^{-sq/10}}\right] \simeq \log\gamma, \tag{4.111}$$

where the $\simeq$ should be a reminder, that equality only holds in the aforementioned limit. The difference of the quantities can now be calculated to be $\log[\frac{2\sqrt{e}}{\pi}] \approx 0.07$. This shows that asymptotically, the estimation of the max-entropy via the function γ gives no significant reduction in the key rate.

4.5.3. Comparison with collective attacks

After having given the security proof in the previous section and calculating expected key rates against general, coherent attacks, we will now describe how to estimate the security in the case of collective Gaussian attacks. In this case, we can use a different strategy than for coherent attacks. Under collective attacks, the state of Alice and Bob is the same in every instance of the protocol, so they are able to perform state tomography. Then, using the fact that the attacks are Gaussian, they can estimate the displacement and covariance matrix of the state and construct the purification of the state. This purification can then be used to bound the information of the eavesdropper. We can then further estimate the min-entropy in the key length formula via the von Neumann entropy using the asymptotic equipartition theorem (AEP). The results of this section have also been published in [FFB+12], where the technical parts are contained in the appendix.

The protocol in case of collective Gaussian attacks is basically the same as in the case of coherent attacks. Both parties will again perform measurements at random and the key will be generated from amplitude and phase measurements. They are in principle free to choose further measurements for the state estimation. We will for now not specify on a specific estimation procedure but just assume that it will reconstruct a state from a certain confidence set $\mathcal{C}_{\epsilon_{PE}}$, except with probability $1-\epsilon_{PE}$. We note, that we will assume that the state is a squeezed vacuum state. We denote the number of transmitted signals n and the number of signals used for the tomography by k. In contrast to the case of collective attacks, there is no need for a restriction of the possible outcomes. For any realistic detector, there will certainly be an upper limit, but we will not be concerned with this in the following. This also implies that the protocol may give a zero key rate, but will never abort.

Theorem 4.5.1. *In a protocol described above and under the assumption of collective Gaussian attacks, an ϵ_s-secure and ϵ_c-correct key of length l can be extracted, provided that not more then l_{EC} bits have leaked during error correction, where*

$$l \leq n \inf_{\Gamma \in \mathcal{C}_{\epsilon_{PE}}} H(X_A|E) - \sqrt{n}\Delta - l_{EC} - \log \frac{1}{\epsilon_1^2 \epsilon_c}, \tag{4.112}$$

where the inf *is taken over the confidence set corresponding to the measurement, $\epsilon \leq (\epsilon_s - \epsilon_1)/(2)$ and*

$$\Delta = 4\log(2^{\frac{1}{2}Hmax(X_A)+1}+1)\sqrt{\log\frac{8}{(\epsilon_s-\epsilon_1)^2}}. \tag{4.113}$$

Proof. Starting point of the proof is again the key length formula (4.2.24), where the task is to bound the smooth min-entropy $H^{\epsilon}_{\min}(X_A|E)$. But under the assumption of collective attacks, we can directly apply the AEP (4.2.12), which gives

$$H^{\epsilon}_{\min}(X^n_A|E^n) \leq nH^{\epsilon}_{\min}(X_A|E) - \sqrt{n}4\log(2^{\frac{1}{2}H\min(X_A|E)}+2^{\frac{1}{2}H\max(X_A|E)}+1)\sqrt{\log\frac{2}{\epsilon}}. \tag{4.114}$$

In order to simplify the expression, we use the following estimations:

$$\begin{aligned} H_{\max}(X_A|E) &\leq H_{\max}(X_A) &(4.115)\\ -H_{\min}(X_A|E) \leq H_{\max}(X_A|C) &\leq H_{\max}(X_A), &(4.116)\end{aligned}$$

where the two inequalities on the right follow from the data processing inequality 4.2.10 and the first inequality for the min-entropy is the duality relation which holds for arbitrary purifications (C is an auxiliary system). With these estimations it follows that

$$2^{\frac{1}{2}H\min(X_A|E)}+2^{\frac{1}{2}H\max(X_A|E)} \leq 2^{\frac{1}{2}H\max(X_A)+1}, \tag{4.117}$$

which proves the form of δ. To complete the proof we observe, that the minimum over the von Neumann entropy for states with the same second moments is attained for Gaussian states. This principle can be found in [GPC06, NGA06]. □

In Fig. 4.2 we have plotted the secure key rate against collective attacks using (4.112). We see, that compared to the coherent attacks, under collective attacks the expected key rate is higher, as is the robustness against noise. In the given parameter range, a positive key rate was obtainable up to 25% additional loss.

For our analysis we chose a model for the confidence set where every entry of the covariance matrix is varied with a $\sqrt{n}$ fluctuation, i.e.,

$$\mathcal{C}_{\epsilon_{pe}} = \left\{\tilde{\Gamma}|\tilde{\Gamma} \in \left[\Gamma_{ij}(1-\frac{f(\epsilon_{pe})}{\sqrt{n}}), \Gamma_{ij}(1+\frac{f(\epsilon_{pe})}{\sqrt{n}})\right]\right\}, \tag{4.118}$$

where $f(\epsilon_{PE})$ gives the desired confidence. In the Gaussian case the function is derived e.g. in [LGG10] and scales such that $\mathrm{Erf}(f) = 1-\epsilon_{pe}$, where Erf is the error function.

To complete the analysis, we will now compare the collective and coherent case with the asymptotic limit derived from the Devetak-Winter bound. We have seen in section 4.2.6, that this bound in our case takes the form

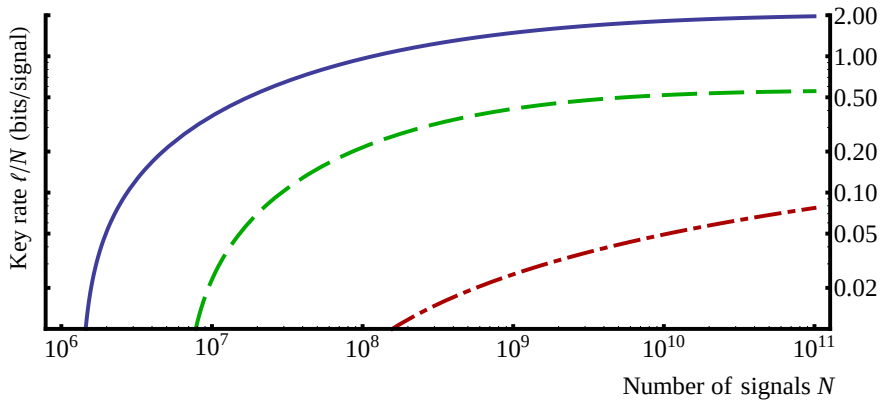

Figure 4.2.: Extractable key rate against number of sent signals for different values of loss under the assumption of collective Gaussian attacks: 0% (blue solid line), 15% (green dashed line) and 25% (red dot-dashed line). Input squeezing was 11 dB and anti-squeezing 16 dB. The excess noise was set to 1% and the security parameters to $\epsilon_s = \epsilon_c = \epsilon_{pe} = 10^{-6}$ and the error correction efficiency $\beta = 95\%$.

$$r_{\mathrm{DW}} = \beta I(X_A;X_B) - I(X_A;E). \tag{4.119}$$

It is also clear from the construction that the bound obtained for collective attacks will converge to the Devetak-Winter bound in the limit of infinite repetition.

In Fig. 4.3 we compared the key rates for coherent, collective and asymptotic for a fixed number of 10^9 signals. We see again that the coherent rate is much worse then the rates obtained under the assumption of collective attacks and in the asymptotic limit.

4.6. Discussion and Outlook

In this chapter we presented a new technique to proof security of a continuous variable QKD protocol. Our technique is based on the entropic uncertainty relation and allowed us to predict a positive key rate for today feasible experiments that are secure against coherent attacks. The secure key rates obtained from our proof do, however, not converge to the Devetak-Winter bound in the limit if infinite repetition. When considering the similar proof technique in the finite dimensional case, this would be the case, so one should search to improve the estimation.

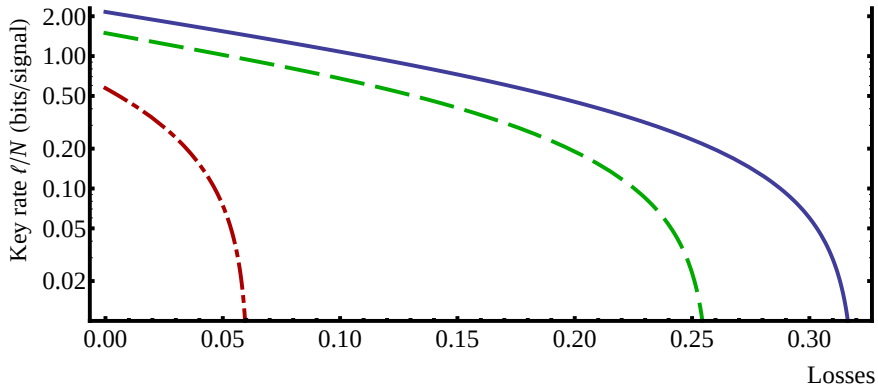

Figure 4.3.: Extractable key rate against added noise for the Devetak-Winter rate (blue solid line), collective attacks (green dashed line) for 10^9 signals and coherent attacks (red dot-dashed line) for 10^9 signals. Input squeezing was 11 dB and anti-squeezing 16 dB. The excess noise was set to 1% and the security parameters to $\epsilon_s = \epsilon_c = \epsilon_{pe} = 10^{-6}$ and the error correction efficiency $\beta = 95\%$.

In our scheme there were two important estimations: first we used the uncertainty relation to estimate the min-entropy, and second we used an explicit construction to estimate the max-entropy as a function γ, only dependent on the observed differences in the measurement results. We have further seen, that the second estimation is asymptotically only by 0.07 bits below the optimum, which indicated that there is not much room for improvement here. To improve our bound, one should thus try to improve the entropic uncertainty relation in our case. The uncertainty relation as presented here is tight in general, but there is no reason, why it should be tight for the squeezed states under consideration. One should thus try to find a state dependent version of the uncertainty relation which can improve the bound under realistic, and testable assumptions.

In order to apply the uncertainty relation, we had to use an estimation to effectively truncate the state on the region that is seen by the detectors. More precisely, we needed to bound the probability that any measurement value lies outside this region. To make this estimation, we chose to place the source in Alice's lab, which simplified the estimation. It would be interesting to derive bounds, which are not dependent on this assumption. Unfortunately, placing the source in Alice's hand is probably the strongest requirement, so any different estimation will probably further reduce the key rate.

The way we did the overall estimation had the advantage, that only assumptions about Alice's lab enter the estimation. We calculated the rates under the assumption, that Alice is in every round able to perform position or momentum measurement without error in the basis choice. When an actual experiment is involved, this is not realistic, but one would have to include a deviation from the ideal situation in the calculation of the constant c in the uncertainty relation.

In the study of Gaussian QKD, one needs extra tools to break the "3 dB loss limit". This can either be accomplished with post selection [SRLL02] or reverse reconciliation [GG02]. Both techniques are not compatible with our proof scheme. The post selection would require to ignore certain parts of the outcomes, which would conflict with the use of the uncertainty relation, i.e., which would make the estimation trivial. The reverse reconciliation on the other hand is not compatible with the fact that the source has to be located in Alice's lab. It would be interesting to investigate, under which circumstances a version of the entropic uncertainty relation is possible that is compatible with post selection.

Finally we note, that in the presentation we used a highly symmetric situation, applying the same loss on both sides and only considering states with an amplitude/phase symmetry. If one drops these assumptions, one needs to introduce more free parameters in the optimization. The cut-off parameter α and the discretization parameter δ will then be optimized separately for Alice and Bob, and position and momentum.

We further note that, though not part of this thesis, to the best of our knowledge there are no off-the-shelf implementations for error correction codes in the required parameter regime available. These will have to be created to make the scheme applicable in practice.

5. Extremal Quantum Correlations

Overview and Contributions

In this chapter we will investigate device independent cryptography from a general perspective and show that in an error free scenario device independent security is equivalent to the extremality of the observed probability distributions. This work was performed in collaboration with F. Furrer and R.F. Werner in the quantum information group in Hannover. Results were published in [FFW11].

5.1. Introduction

The main virtue of quantum cryptography lies in the fact, that quantitative bounds can be given on the amount of information that has leaked to the environment during communication and, hence, to any eavesdropper. These security considerations, however, are usually based in a specific framework, i.e., under certain assumptions concerning the preparation and the measurements that are used. For example in the historically first implementation, the BB84 protocol[BB84], one assumption was that the legitimate parties transmit only single qubits.

There are actually two assumptions included here, namely first that in each transmission event only a single indivisible system is generated and second that this system has Hilbert space dimension 2. If either of the two conditions is dropped, the protocol becomes insecure: information about the basis choice of the bit value might be accessed from parts of the signal that are not visible to Bob, thus, compromising the security (see e.g. [Lüt00, SBPC$^+$09]). Some of these assumptions can be dropped, by employing a different protocol, e.g., a decoy state protocol to remove the assumption of single systems ([Hwa03], for a review see also [SBPC$^+$09]).

It was realized, that quantum mechanics might, at least in principle, offer ways to circumvent a wide range of such assumptions by employing appropriate tests and ultimately arrive at a level of security that is independent of the proper functioning of the devices used. This idea was put forward first under the term of self testing devices in [MY98] and applied to QKD in quantitative form in a security proof against collective attacks in [ABG$^+$07]. In both cases, the test was based on a violation of the CHSH inequality.

The intuition behind the proof is as follows: First observe that if two parties

share a pair of maximally entangled qubits, they are able to maximally violate the CHSH inequality using appropriate measurements. But moreover, the converse is also true, i.e., whenever a maximal violation of a CHSH inequality is observed, the states that are present must be located on a qubit subspace and on this subspace form a maximally entangled pair. This also implies that the results from such measurements are uncorrelated from any other measurement, especially of those of an eavesdropper. In this case we also say that the correlation are independent from the eavesdropper.

In the literature, device independent QKD was first proven secure against collective attacks in [ABG+07] and later generalized to commuting measurements [HR10] and causally independent measurements [MPA11]. For an overview on the first years of device independence and extensions to general non-signaling theories we also refer to [Hän10].

Our main motivation is to identify the origin of this independence and whether it is a special feature of the CHSH inequality or a generic feature of all Bell inequalities. We are thus not interested in a specific protocol, but want to answer the question for a general situation with an arbitrary (but finite) number of participants, measurements and outcomes. In section 5.3, we find that perfect independence from third party measurements is given if and only if the corresponding probability distribution of outcomes is extremal in the set of all probability distributions. Concerning the initial question, this implies that any unique maximal violation of a Bell inequality implies extremality of the underlying probability distribution, and thus, independence of external measurements. Conversely, there are extremal probability distributions that offer perfect independence without a maximal violation of a Bell inequality. The connection between extremality and security has also been studied in the context of general non-signalling theories [BLM+05] and applied for a bipartite situation under the assumption of individual attacks in [BHK05].

In section 5.4, we will further study a stronger notion of independence, we named algebraic security, which is connected to the uniqueness of the representation of the system under consideration. We will consider examples in section 5.5 and show that in certain cases, security also implies algebraic security.

Our study of extremal correlations and their connection to cryptography was performed in collaboration with F. Furrer under the supervision of R.F. Werner at the University of Hannover and published in [FFW11]. We thank V. Scholz and D. Gross for useful discussions.

5.2. Correlation tables and quantum representations

We consider an arbitrary statistical experiment conducted by N honest parties that are at distinguishable locations and collaborate to perform the experiment. In every

run of the experiment, each experimenter chooses a specific measurement from a set of measurement devices and observes a measurement result from a set of possible outcomes defined by the measurement device in use. During the run of the experiment, all experimenters are considered to be independent from each other, particularly in their choices of measurements. When the experiment has been conducted, the acquired data is brought together and a the probability distributions $\mathbb{P}$ of outcomes are determined which will be the objects of study in the remainder of the chapter.

One should note here, that in a general situation, the number of measurement devices could be different from experimenter to experimenter and likewise the number of possible results could be different for all measurement devices. We will restrict to a symmetric situation to keep the notation short. The technical results do not depend on this and can be generalized to the asymmetric situation. We further restrict to finite discrete sets of measurements and outcomes. We will comment at the end of the chapter on the possibilities of dropping this assumption.

Definition 5.2.1. *In the following we always assume an experiment conducted by N parties, with M possible measurement devices and K outcomes, which we will call the (N,M,K) situation. We will call the measurement setting of the i-th party s_i and the outcomes x_i, where $i \in [1,N]$, $s_i \in [1,M]$ and $x_i \in [1,K]$. We further denote the collection of all settings for a specific run by $\underline{s} = (s_1, s_2, ..., s_N)$ and of all outcomes by $\underline{x} = (x_1, x_2, ..., x_N)$. Then the probability for obtaining an outcome $\underline{x}$ while given a setting $\underline{s}$ is denoted by $\mathbb{P}(\underline{x}|\underline{s})$. The normalization condition gives that $\sum_{\underline{x}} \mathbb{P}(\underline{x}|\underline{s}) = 1$ for all $\underline{s}$.*

One should however note, that not all these probability distributions can actually be realized by quantum mechanics with independent measurements as required above. To do so, one first needs to discard all probability distributions that allow signaling, i.e., for which the outcome of a part depends on the measurement setting of another. Formally this non-signalling condition demands that $\mathbb{P}(x_i|s_i) = \mathbb{P}(x_i|\underline{s})$ for all $i, x_i, \underline{s}$. We denote the set of all probability distributions that fulfill the no-signalling condition by $\mathcal{P}$. It is known, that the no-signaling set is a polytope, and that it is strictly larger then the set obtainable by quantum means.

A smaller set is the one that can be realized with a classical local hidden variable model. This set also forms a polytope, its extreme points are points with a deterministic assignment of outcomes. We denote this set by $\mathcal{C}$. The faces of maximal dimension of this polytope correspond to proper Bell inequalities. The structure of this polytope can in principle be constructed, and classifications are known for systems up to a certain degree. A survey on the topic together with a more detailed collection of known results and references can be found online in the list of open problems in quantum information [QIP]. The $(2,2,2)$-case is known to have an exceptionally simple structure, as all Bell inequalities are equivalent to the CHSH-

inequality [Fin82]. General constructions for the classical polytope are known in some cases. A complete description of the $(N,2,2)$ has been presented in [WW01]. For a review on general constructions, we refer to [PLZ06].

We are now interested in all probability distributions that can be realized within quantum mechanics, denoted by $\mathcal{Q}$. These distributions are said to have a quantum representation in the following sense:

Definition 5.2.2. *A probability distribution $\mathbb{P}(\underline{x}|\underline{s})$ admits a quantum representation if there exists: a Hilbert space $\mathcal{H}$, POVMs $\{F_i(x_i,s_i)\}$ and a state $\omega : \mathcal{B}(\mathcal{H}) \to \mathbb{C}$ such that*

$$[F_i(x_i,s_i),F_j(x_j,s_j)] = 0 \quad \forall\, i \neq j \tag{5.1}$$

and

$$\mathbb{P}(\underline{x}|\underline{s}) = \omega(F(\underline{x}|\underline{s})), \tag{5.2}$$

where $F(\underline{x}|\underline{s}) = F_1(x_1|s_1)\cdot ... \cdot F_N(x_N|s_N)$. We denote this as $(\mathcal{H},\omega,\{F_i\})$-representation.

Let us first note that there is a strict inclusion of the sets, namely $\mathcal{C} \subset \mathcal{Q} \subset \mathcal{P}$. We summarize a few geometrical facts about $\mathcal{Q}$: first, it is convex, but not a polytope. In contrast to $\mathcal{C}$, which was defined by finitely many Bell inequalities, the boundary of $\mathcal{Q}$ cannot be defined by any finite number of linear inequalities. Nevertheless, any extreme point of $\mathcal{Q}$ maximizes a linear inequality, which we call a Tsirelson inequality. This nomenclature corresponds to the most famous CHSH case, in which the maximal value of the CHSH functional in $\mathcal{C}$ is given by 2 [CHSH69], while the maximal value allowed by quantum mechanics is $2\sqrt{2}$, as shown by Tsirelson [Tsi80]. In this sense, every Bell inequality defines a Tsirelson inequality, while conversely every Tsirelson inequality defines a generalized Bell inequality, though not necessarily a proper one. There are points, for which the generalized Bell and the Tsirelson inequalities give the same bound, e.g., the classical deterministic points.

For a given Bell inequality, the problem of finding the maximal value within $\mathcal{Q}$ can be solved via a hierarchy of semi-definite programs [DLTW08, NPA08]. The use of this hierarchy is in principle always possible, although the resources needed for the optimization do not scale efficiently. We remark, that it can also be helpful to consider non-linear inequalities for the study of $\mathcal{Q}$. In [Mas03] this was done to give a complete characterization of all full correlation tables in $\mathcal{Q}$ in the $(2,2,2)$-case.

From the definition of a quantum representation 5.2.2 it is in general possible to find different representations for the same probability distribution. An obvious construction method for a equivalent representation is to connect the representations with a unitary transformation. We will in the following say that two quantum representations are equivalent, if they can be connected with a unitary transformation. We will next show how to use a version of the Stinespring theorem [Sti55, Pau02] to find a dilation of a given state into standard form.

Theorem 5.2.3. *For any quantum representation $(\mathcal{H},\omega,\{F_i\})$ there exists a representation $(\tilde{\mathcal{H}},\rho,\{\tilde{F}_i\})$, where the $\{\tilde{F}_i\}$ are projection operators, $\rho=|\Omega\rangle\langle\Omega|$ is a pure state cyclic for the algebra generated by the projections $\mathcal{A}(F)$ such that*

$$\mathbb{P}(\underline{x}|\underline{s})=tr(\rho\,\tilde{F}(\underline{x}|\underline{s})). \tag{5.3}$$

Here, cyclic means, that $\overline{\{G|\Omega\rangle|G\in\mathcal{A}(F)\}}=\mathcal{H}$.

Proof. The proof is performed by explicit construction and is similar to the construction used in the GNS-construction [BR79]. It has been presented previously, e.g., in the supplement of [FFW11].

Starting from the given representation $(\mathcal{H},\omega,\{F_i\})$, one first uses a version of the Naimark dilation theorem to make the measurements projective. It suffices to show this procedure for one of the observables on one of the sites and to ensure that projectivity of the other observables is preserved. Then this technique can be applied to all observables on all sites successively. Consider without loss, the observable $\{F_1(x|1)\}_x$. Define $\widehat{\mathcal{H}}=\bigoplus_{i=1}^{K}\mathcal{H}$ and P_x as the projection on the x-th summand. Define further the isometry

$$V:\mathcal{H}\to\widehat{\mathcal{H}}\quad\text{s.th.}\quad V\phi=\bigoplus_{i=1}^{K}\sqrt{F_1(x,1)}\phi. \tag{5.4}$$

Now set

$$\hat{F}_1(x|s)=\begin{cases} P_x & s=1\\ VF_1(1,s)V^*+(\mathbb{1}-VV^*) & s\neq 1,x=1\\ VF_1(x,s)V^* & s\neq 1,x\neq 1\end{cases}. \tag{5.5}$$

As V is an isometry, i.e., $V^*V=\mathbb{1}$, one directly sees that $V^*\hat{F}_1(x|s)V=F_1(x|s)$ and that projective measurements remain projective. For all other sites ($j\neq 1$), we set $\widehat{F}_j(x|s)=\bigoplus_x F_j(x|s)$. It follows, that $\widehat{F}_j(x|s)V=VF_j(x|s)$, and with this, we see that the $\widehat{F}_j$ commute for different j and so the product can be unambiguously defined. Setting $\widehat{\omega}(\cdot)=\omega(V\cdot V^*)$ we obtain a representation with projective measurements.

The fact that the state can be chosen pure and cyclic is a direct consequence of the GNS-construction (A.1.3). □

Now we have gathered the ingredients to state the definition of security and to discuss the connection to quantum representations.

5.3. Cryptographic setting

We have seen in the previous subchapter how probability distribution are represented within quantum mechanics. Now, we are interested in the cryptographic

setting. The question here is, how much information about the measurement results of the legitimate parties can be inferred by an eavesdropper. As usual, the eavesdropper may perform any operation permitted by quantum mechanics and has arbitrary resources, but is not allowed to interfere with the laboratories. The property of not being able to interfere with the laboratories is modeled by choosing the measurement operators of the eavesdropper commuting to the legitimate parties. An important assumption we make here is, that the probability distributions are known without error. This condition is not realistic, as it can never be achieved in an experiment. We will comment on the possibility to circumvent this restriction at the end of the chapter.

In addition to the measurements on his part of the system, the eavesdropper has full prior knowledge about the outcome statistics of the system, i.e., full knowledge about the probability distribution $\mathbb{P}$. This means, that if the outcomes are not equally distributed, he can utilize this prior knowledge. In the extreme case of deterministic points, he would obtain full information about the outcomes in every run without performing any measurement at all. These cases can however be accounted for, as the legitimate parties are always assumed to know $\mathbb{P}$. In the following we will thus be interested in deciding whether the eavesdropper can gain additional information by performing measurements.

All legitimate parties and the eavesdropper will be modeled by quantum systems, where the fact that the eavesdropper has no direct access to their laboratories is modeled by choosing the measurement operators forming her POVM $\{E_y\}$ commutung with all the operators of the legitimate parties, i.e., $[E_y, F_i(x|s)] = 0$.

Let us note here, that it is an open question, whether this commutation requirement is equivalent to modeling the eavesdropper on a different tensor factor then the legitimate parties, where the later condition clearly implies the former. These notions are known to be equivalent if the underlying system has finite dimensions but the answer to the general question, called the "Tsirelson conjecture", is still open. It has been shown to be equivalent to open problems in algebra, like the "Kirchberg conjecture" and "Connes' embedding problem". For further reading on this topic we refer to [SW08, JNP$^+$11].

Definition 5.3.1. *We say that the probability distribution $\mathbb{P}$ is independent of the eavesdropper, if for any quantum representation $(\mathcal{H}, \omega, \{F_i\})$ and any positive operator E_y with $[E_y, F_i(x|s)] = 0$ for all i it holds that*

$$\omega(E_y F(\underline{x}|\underline{s})) = \omega(E_y) \cdot \omega(F(\underline{x}|\underline{s})) = \omega(E_y) \cdot \mathbb{P}(\underline{x}|\underline{s}). \tag{5.6}$$

As argued above, this independence condition is trivially satisfied for all classical deterministic points. We will thus refine the definition to exclude these trivial cases.

Definition 5.3.2. *We say that a probability distribution contains security if it is independent and not of product form, i.e., $\mathbb{P}(\underline{x}|\underline{s}) \neq \prod_{i=1}^{N} \mathbb{P}(x_i, s_i)$.*

The amount of extractable security in the probability distribution is then given by the prior distributions of outcomes, and maximal if the outcomes are equally distributed. As we are only interested in deciding, whether a probability distribution contains any security, and to use the same notation as [FFW11], we will call a probability distribution secure, if it contains security.

Let us compare this to the situation in chapter 4. Here, the main ingredient for the security proof of QKD protocols was the privacy amplification theorem which stated how much information was contained in a distribution held by Alice, when considering the quantum system of the eavesdropper. The theorem was thus formulated for a bipartite Alice/Eve split, while in the actual protocol Alice and Bob need to perform additional error correction to make their outcome strings equal while loosing bits in the process. The maximal information Alice could extract this way was given by the min-entropy, which was given as the guessing probability for an optimal measurement strategy by Eve. The situation here is per definition a multi-party situation that was formulated without respect to any error correction. In fact, there is no guarantee that the secure N-party probability distributions contain sufficient correlations, so there could be situation in which Eve is uncorrelated, i.e., does not learn by measurements, but the legitimate parties might still not be able to extract any key. If definition 5.6 is fulfilled, we already know that the optimal guessing strategy for Eve is given by the maximal value in the prior probability distribution and we would thus be able to bound the min-entropy between Eve and the legitimate parties, but we do not get an estimation for the leakage term that appears in the error correction.

After these definitions, we can now state the characterizing theorem:

Theorem 5.3.3. *A probability distribution contains security, if and only if it is extremal and not classical, i.e., extremal in $\mathcal{Q}\backslash\mathcal{C}$.*

Proof. We first show that security implies extremality. Suppose, $\mathbb{P}$ is secure but not extremal. Then there exist a convex decomposition $\mathbb{P} = \lambda\mathbb{P}_1 + (1-\lambda)\mathbb{P}_2$ with $\lambda \in [0,1]$. Now choose a direct sum representation for $\mathbb{P}_1$ and $\mathbb{P}_2$. This means we choose representations $(\mathcal{H}_j, \omega_j, F_j(\underline{x}|\underline{y}))$ and $\mathcal{H} = \lambda\mathcal{H}_1 \oplus (1-\lambda)\mathcal{H}_2$, $F(\underline{x}|\underline{y}) = \lambda F_2(\underline{x}|\underline{y}) + (1-\lambda)F_2(\underline{x}|\underline{y})$. Choose $E_{1/2}$ as the projector on the respective summand. One checks, that these commute with the measurements $[E_j, F(\underline{x}|\underline{y})] = 0$. Then the condition (5.6) directly gives, that $\mathbb{P} = \mathbb{P}_1 = \mathbb{P}_2$, so the decomposition is indeed trivial and $\mathbb{P}$ is extremal. As we have explicitly excluded product form for $\mathbb{P}$ in the definition of security and all extremal correlations in $\mathcal{C}$ are of product form, it it is clear that $\mathbb{P}$ is not in $\mathcal{C}$.

Conversely, suppose $\mathbb{P}$ is extremal in $\mathcal{Q}\backslash\mathcal{C}$. First observe, that, as $\mathbb{P}$ is extremal and not in $\mathcal{C}$, it cannot be of product form. Choose an arbitrary operator E commuting

with the $F(\underline{x}|\underline{s})$ and set $\lambda = \omega(E)$ and

$$\mathbb{P}_1(\underline{x}|\underline{s}) = \frac{1}{\lambda}\omega(E \cdot F(\underline{x}|\underline{s})) \tag{5.7}$$

$$\mathbb{P}_2(\underline{x}|\underline{s}) = \frac{1}{1-\lambda}\omega\left((\mathbb{1} - E) \cdot F(\underline{x}|\underline{s})\right). \tag{5.8}$$

Then it follows that $\mathbb{P}(\underline{x}|\underline{s}) = \omega(F(\underline{x}|\underline{s})) = \lambda\mathbb{P}_1(\underline{x}|\underline{s}) + (1-\lambda)\mathbb{P}_2(\underline{x}|\underline{s})$. But $\mathbb{P}$ is extremal, so the decomposition must be trivial and $\mathbb{P} = \mathbb{P}_1 = \mathbb{P}_2$. But then equation (5.7) is exactly the independence condition (5.6). □

This theorem links the definition of uncorrelated, or secure, probability distributions to the geometric property of extremality. Unfortunately, the characterization of all extremal correlation tables, or even the certification of extremality is no easy task, even in a scenario with small (N, M, K). One way of certifying extremality is to show that a given probability distribution maximizes a non-trivial Tsirelson inequality, which can be done via a hierarchy of semi-definite programs [NPA08], which becomes impractical also for small (N, M, K). As a second direct consequence, one sees that the requirement in definition 5.3.1 that independence should hold for "any" quantum representation of the probability distribution is actually not severe as with theorem 5.3.3 independence of one representation automatically implies independence for any other representation.

5.4. Algebraic security

We now come to a strengthened definition of security. Where in the previous section we were interested in certifying independence for all measurement operators necessary to determine the given probability distribution, we turn our attention now to the complete algebra generated by these operators.

Definition 5.4.1. *For a given set of positive operators $\{F_i\} \in \mathcal{B}(\mathcal{H})$, we denote by $\mathcal{A}(F)$ the algebra generated by the operators, i.e., the smallest closed $*$-subalgebra of $\mathcal{B}(\mathcal{H})$ containing the F_i.*

This definition makes explicit reference to a specific representation of the probability distribution. We will denote the direct sum of all inequivalent representations of $\mathbb{P}$ as $U(\mathbb{P})$, and the set of all possible representations of all possible probability distributions for a given (N, M, K)-setting as $U(N, M, K)$. This set is also called the universal C^*-algebra for the (N, M, K)-case.

We now introduce a stronger notion of independence, where we follow in our nomenclature again [FFW11].

Definition 5.4.2. *We call a probability distribution algebraically secure, if it does not factorize, and for any operator E commuting with the $F_i(\underline{x}|\underline{s})$ and any operator $\tilde{F}(\underline{x}|\underline{s}) \in \mathcal{A}(F)$ it holds that*

$$\omega(E \cdot \tilde{F}(\underline{x}|\underline{s})) = \omega(E) \cdot \omega(\tilde{F}(\underline{x}|\underline{s})). \tag{5.9}$$

This property can be related to algebraic uniqueness, which means that for the probability distribution, any two quantum representations are unitarily equivalent.

Theorem 5.4.3. *A probability distribution is algebraically secure if it is algebraically unique, i.e., extremal in $\mathcal{Q}\backslash\mathcal{C}$ and has a unique representation.*

We note here, that the definition of algebraic uniqueness is equivalent to the condition that $U(\mathbb{P})$ consists of only one direct summand.

Proof. First, suppose that the distribution is algebraically secure. We need to show, that all representations are unitarily equivalent. Let $(\mathcal{H}_1, \omega_1, F_1(\underline{x}|\underline{s}))$, $(\mathcal{H}_2, \omega_2, F_2(\underline{x}|\underline{s}))$ be two representations in standard form. Then the extremality condition (5.9) evaluated for $\tilde{F}_1 \in \mathcal{A}(F_1)$ and $\tilde{F}_2 \in \mathcal{A}(F_2)$ gives that $\omega_1(\tilde{F}_1) = \omega_2(\tilde{F}_2)$. Otherwise, the direct sum representation evaluated with E chosen as projector on the first or second summand will give a contradiction. Next we use that in standard form, the states are pure and define the unitary operator $U : \mathcal{H}_1 \to \mathcal{H}_2$ as $U\tilde{F}_1|\Omega_1\rangle = F_2|\Omega_2\rangle$. Because the states are cyclic for their respective spaces, this implies that U can be extended to the whole space and thus, the representations are unitarily equivalent. As the representations have been arbitrary, this means that all representation are unitarily equivalent.

To show the converse, suppose, the probability distribution is algebraically unique. Consider an arbitrary $0 \leq E \leq \mathbb{1}$, commuting with the $F(\underline{x}|\underline{s})$. We define the state $\tilde{\omega}$ as $\tilde{\omega}(A) = \frac{1}{\omega(E)}\omega(\sqrt{E}A\sqrt{E})$. Since $\mathbb{P}$ is extremal, this state together with the operators $F(\underline{i}|\underline{s})$ is a valid quantum representation of $\mathbb{P}$. But then E is equivalent to $\mathbb{1}$, which implies 5.9. As E was chosen arbitrary, this means that the state is algebraically secure. □

Let us discuss the relation between security and algebraic security from a geometrical point of view. Fundamental objects are two convex sets, the set of all quantum representations, which we denote by $\mathcal{S}$, and the set of all probability distributions $\mathcal{Q}$. We can formally introduce the map $\Gamma : \mathcal{S} \to \mathcal{Q}$ that maps every quantum representation to its corresponding probability distribution. We know, that this map is linear, surjective, i.e., every quantum probability distribution has a representation, but not injective, i.e., not every representation is unique. As mentioned above, the geometric structure of $\mathcal{Q}$ and $\mathcal{S}$ is in general not known. in particular, the existence of faces cannot be excluded in higher dimensions. In fact, in the $(3,2,2)$-case, the set $\mathcal{Q}$ has a face, i.e., there exist a proper Bell inequality without quantum violation, which was shown in [ABB+10].

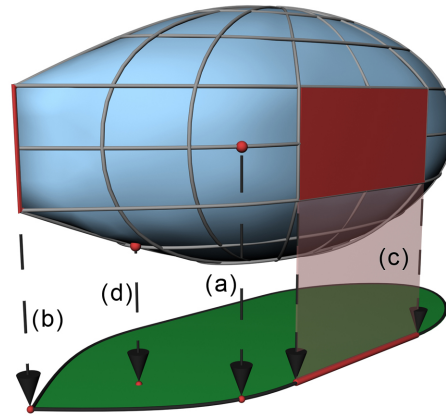

Figure 5.1.: Sketch of the set of quantum representations $\mathcal{S}$ (above) and the set of probability distributions $\mathcal{Q}$ (below). An extremal probability distribution can either correspond to a unique point (a) or to a face of $\mathcal{S}$ (b). Other faces of $\mathcal{S}$ can be mapped to faces of $\mathcal{Q}$ (c). Not all extremal points of $\mathcal{S}$ are also extremal for $\mathcal{Q}$ (d).

The possible configurations are visualized in Fig. 5.1 (which has also been presented in [FFW11]). First, there is the possibility that a single extremal point of $\mathcal{S}$ is mapped to an extremal point $\mathbb{P} \in \mathcal{Q}$. In other words, the inverse $\Gamma^{-1}(\mathbb{P})$ is a single point. Then $\mathbb{P}$ is algebraically secure (this corresponds to point (a) in Fig. 5.1). Other extreme points of $\mathcal{Q}$ can correspond to a face of $\mathcal{S}$, in which case the point is secure, but not algebraically secure (b). One should further note, that not all points in the boundary of $\mathcal{Q}$ are extreme points, as the boundary of $\mathcal{Q}$ can have faces (c), and that not all extreme points of $\mathcal{S}$ are mapped to boundary points in $\mathcal{Q}$ (d).

5.5. Examples

The (N,2,2) case

A situation that is well understood is the $(N,2,2)$-case, i.e., the N party situation with two dichotomic observable per site. For reference see e.g. [RS89, WW01, Mas05]. In this case, all irreducible quantum representations are equivalent to an N-qubit representations. That is, the Hilbert space is given as $\mathcal{H} = \bigotimes_{i=1}^{N} \mathbb{C}^2$ with an arbitrary pure state $|\psi\rangle \in H$. The measurement operators on each of the tensor factors are parameterized by a single angle θ_i. They can be chosen as

$$F(1|1) = \frac{1}{2}(\mathbb{1}+\sigma_z) \tag{5.10}$$

$$F(2|1) = \frac{1}{2}(\mathbb{1}-\sigma_z) \tag{5.11}$$

$$F(1|2) = \frac{1}{2}(\mathbb{1}+\sin(\theta_i)\sigma_x+\cos(\theta_i)\sigma_z) \tag{5.12}$$

$$F(2|2) = \frac{1}{2}(\mathbb{1}-\sin(\theta_i)\sigma_x-\cos(\theta_i)\sigma_z), \tag{5.13}$$

where the $\sigma_{x/z}$ denote the corresponding Pauli matrix. With this, any correlation table in $\mathcal{Q}(N,2,2)$ is defined by the state $|\psi\rangle$ and the N angles $\{\theta_i\}$. Note here, that any non-irreducible representation can be written as direct sum of at most 4^N+1 irreducible quantum representations.

Extremality can now be certified, if one can show that the given probability distribution maximizes a Tsirelson inequality. This Tsirelson inequality, or functional, $\tau : \mathcal{Q} \to \mathbb{R}$, is specified by a set of coefficients $\{c(\underline{x}|\underline{s})\}$ as $\tau(\mathbb{P}) = \sum_{\underline{x},\underline{s}} c(\underline{x}|\underline{s})\mathbb{P}(\underline{x}|\underline{s})$. Then the maximal value of the Tsirelson inequality is given by

$$Q_c = \max_{\mathbb{P}\in\mathcal{Q}} \tau(\mathbb{P}) = \max_{\mathbb{P}\in\mathcal{Q}} \sum_{\underline{x},\underline{s}} c(\underline{x}|\underline{s})\mathbb{P}(\underline{x}|\underline{s}). \tag{5.14}$$

If one has found such a maximizing $\mathbb{P}$, in order to show extremality one further needs to assure, that $\mathbb{P}$ is not inside a face. A maximum can in general be calculated using a hierarchy of semi-definite programs, as described in [DLTW08, NPA08]. Using the representation for the $(N,2,2)$ case, we can analyze the optimization problem a bit further. We see that the optimization of 5.14 can be translated into the optimization of a measurement operator C, which is defined as $C = \sum_{\underline{x},\underline{s}} c(\underline{x}|\underline{s})F(\underline{x}|\underline{s})$. By taking the irreducible representation of the corresponding probability distribution, we see that it is determined by the parameters $\theta_1,\ldots,\theta_N$ of the measurement operator. The optimization is then given by

$$Q_c = \max_{\psi,\theta_1,\ldots,\theta_N} \langle\psi|C(\theta_1,\ldots,\theta_N)|\psi\rangle. \tag{5.15}$$

If there is a unique set of parameters $|\psi\rangle, \theta_1,\ldots,\theta_N$ the corresponding probability distribution has a unique representation and is thus algebraically secure. As an example, the Mermin inequalities [Mer90] have a unique maximum in this sense and lead thus to algebraically secure points. If there exists more then one set of maximizing parameters, the corresponding probability distributions and all points in their convex span are secure, but not algebraically secure points.

The (2,M,2) case for full correlations

The extremal correlations in the $(2,M,2)$-case have been analyzed by Tsirelson in [Tsi85]. In this case, the question of deciding extremality can be simplified, if one does not consider general probability distributions, but full correlation tables. We denote the $\{\pm 1\}$-valued measurement operators for Alice by A_i and for Bob by B_i, with $i \in \{1,M\}$. In the notation of the previous chapters, this means e.g. that $A_i = F_A(1|i) - F_A(2|i)$. The set of full quantum correlations $\mathcal{Q}_C$ is then given by correlations $c_{ij} = \mathrm{tr}(A_i B_j \rho)$. It has been proven in [Tsi85] that the study of extremal correlation tables can be simplified, as all extremal correlation tables that are not deterministic have vanishing marginal expectation values, i.e., $\mathrm{tr}(A_i) = 0 = \mathrm{tr}(B_j), \forall i,j, \in \{1,M\}$. This implies that non-deterministic extremal correlation tables in $\mathcal{Q}_C$ are also extremal in $\mathcal{Q}$. Also, extremal correlation tables with unique representation are algebraically secure.

The main tool in the study of extremal correlation tables are c-systems. A c-system is a collection of vectors x_i, y_j, $i,j \in \{1,M\}$ in an Euclidian vector space with dimension M, satisfying $||x_i|| \leq 1, ||y_j|| \leq 1$. It holds, that for every correlation table there exists a c-system with

$$\langle x_i | y_j \rangle = \omega(A_i B_j). \tag{5.16}$$

Observe, that a single correlation table can in general have different, non equivalent c-systems. These c-systems provide an elegant way of studying extremality: for an extremal correlation table, all corresponding c-systems are isometric to each other. Further, $||x_i|| = ||y_j|| = 1$ and the linear hull of the $\{x_i\}$ and $\{y_j\}$ coincide. We call the dimension of these linear hulls the rank of the c-system r. The question of uniqueness of the representation can now be answered in terms of the rank: if the rank is an even number, all representations are equivalent, while if the rank is odd, there are exactly two non-equivalent representations.

With this, the question of extremality can be decided by constructing the corresponding c-system and check the extremality conditions.

5.6. Discussion and Outlook

Our main motivation in this chapter was to clarify, where the security in device independent setup is based on, and whether there is any special role of the CHSH inequality. This led to the definition of independence and security based on the fact that an eavesdropper cannot learn anything about outcomes on the sites of the legitimate parties by measurement. This property was then shown to be equivalent to extremality of the corresponding probability distribution, thus, rephrasing the problem of determining security to the problem of extremality. The proof was general for any number of parties, measurements and outcomes, which shows that the CHSH-inequality has no special role, but is used as a certificate for extremality.

We have noted however, that in general the sets of extremal probability distributions cannot be easily constructed. We have further defined the stronger notion of algebraic security which states that the independence condition has to hold for all operators generated by the measurements of the legitimate parties, and that was linked to the algebraic uniqueness of the probability distribution. Finally we have discussed the connection between the two notions and presented some examples. In summary, we have provided a novel set of tools for the study of device independent cryptography.

Concerning practical applications, however, there are issues not addressed in our work. The first and most serious task is to find bounds on the independence, that also work with a finite accuracy. We have noted, that we only considered probability distributions that are extremal, whereas in a real situation one can only certify a certain distance to an extremal state. If one would want to use our technique for practical estimation of device independent security one needs to say how the independence condition scales in a parameter ϵ, if the probability distribution is at least ϵ-close to an extremal point in an appropriate distance measure. Unfortunately, up to now no practical bounds for this are known. The challenge here is to find a bound that holds for all quantum representations, a problem that is even in the $(2,2,2)$-case not simple.

One possible line of research would be to consider the problem under additional symmetries. It is known, that device independent security bounds in the $(2,2,2)$-case can be obtained when considering only collective attacks [ABG+07] or commuting measurements [HR10]. It would be interesting to understand, whether similar techniques work in a general situation.

As mentioned in the beginning of the section, we have only considered a scenario in which the legitimate parties choose from a discrete set of measurement and are in return given an outcome from again a discrete set. It would be interesting to see, if these restrictions could, in principle, be dropped. Concerning QKD, one should however keep in mind that for any practical communication protocol a digitization at some point is almost unavoidable.

The study of algebraically unique probability distributions is interesting by its own right. The characterization of the state space in higher dimensions and its possible representations has implications for different topics. As far as we know however, even in low dimensional cases, this will involve a massive numerical effort.

6. Conclusion

Investigating ways in which quantum physics can outperform classical physics was the main motivation behind this thesis. We have seen that on the level of single systems this seems not to be the case and even seems that quantum physics is restricted in comparison to classical physics, as certain actions, like disturbance free measurements, are no longer possible. However if one considers systems with two separated parties, it becomes clear that quantum mechanics cannot be seen as "classical mechanics plus some extra rules", instead it permits correlations between the systems that are not compatible with any local classical theory. These quantum correlations can then be used to accomplish tasks like secure key distribution, which is impossible when only only classical communication is permitted.

In **Chapter 3**, we investigated the steering effect - a certain kind of correlation both different from entanglement and the violation of a Bell inequality. Steering describes precisely what was addressed in the original EPR paper. There are two motivations for the study of steering.

It is of fundamental interest to characterize the set of all steering, or equivalently non-steering, states. We have seen that in general the set of all non-steering probability distributions is convex but not a polytope, and is in this respect similar to the set of all quantum correlations. There are a number of questions relating to to the structure of these two sets, i.e., whether a situation can arise in which the boundary of the non-steering set and the quantum set have common non-trivial faces. Unfortunately, no method other than direct construction is known so far for this, and there is little knowledge about the steering properties beyond the two qubit regime. It would be interesting to investigate the three qubit regime and see whether the conjectured monogamy relation holds.

When concerned with Gaussian systems the steering effect can be used as a benchmark for the correlations between the parts of the experiment. In the Gaussian case the violation of a Bell inequality is not possible, while the question whether a state is entangled is possibly not fine enough, hence it is interesting to classify states according to their steering properties. We have seen that in the Gaussian case states can be experimentally realized that display one-way steering, i.e., steering from Alice to Bob but not vice versa. In the case of tripartite steering, we have found an even richer structure of steering, and it would be interesting to see these states realized in an experiment.

In **Chapter 4**, we presented a protocol for continuous variable quantum key distribution. We have proven that it is secure against coherent attacks, composable secure, works in the finite key regime and gives a positive key rate when considering technology that is available today. To the best of our knowledge, this was the first protocol to match all these requirements. The techniques employed are similar to those applied to finite dimensional systems, but in contrast to the finite dimensional case our findings are asymptotically not optimal.

The main feature of the security proof was the possibility to perform privacy amplification, which can be quantified in the finite key regime by the min-entropy. This min-entropy is, except in some special cases, difficult to calculate, so the certification of security is largely equivalent to the estimation of this min-entropy for a given system. We showed how to use a version of the entropic uncertainty relation to estimate the min-entropy by the max-entropy in a situation where Alice and Bob perform homodyne measurements We then showed how to bound the max-entropy by a function that only depends on the observed correlations. We have further seen that asymptotically, this second estimation is close to optimal, hence the difference between the finite key regime and the asymptotic rates for key distribution originates in the entropic uncertainty relation.

To improve the results presented here one could search for a state dependent entropic uncertainty relation that is better suited for the situation under consideration. Second, one needs to improve the estimation on the parameter range of the observed measurements. In our estimation, we placed the source in Alice's lab, while in general it would be desirable to place the source in Eve's hand and to certify the parameter range on observations alone. Placing the source in Eve's hands would also allow the discussion of reverse reconciliation, which could be used to improve the key rate. Additionally it should be checked whether it is possible to make the application of the entropic uncertainty relation compatible with post selection.

In **Chapter 5** we investigated device independent security from a general point of view. We showed how to formulate the notion of security in terms of an independence relation of probability distributions and also that a probability distribution is perfectly secure if and only if it is extremal in the set of all quantum probability distributions. We further introduced the notion of algebraic security and showed that this notion is equivalent to the algebraic uniqueness of an extremal probability distribution. Our findings imply that device independent security is no special feature of the CHSH-inequality, but that conversely any Bell-type inequality can be used to certify extremality.

The main unresolved issue in our approach is, however, that it up to now only holds for extremal probability distribution but not for almost extremal ones. In any practical situation, one would only be able to certify extremality up to a small error, which has to be included in the security analysis. If our approach should be used in a real situation, one would need to extend the theory to provide quantitative

results also for almost extremal correlations. A step before trying to find such bound in general would be to investigate the situation under additional assumptions. A natural assumption would again be, that the legitimate parties are provided with an additional independence promise on their measurements.

The question, how to certify algebraic uniqueness is interesting in its own regard. We have seen that certain correlation inequalities like the CHSH-inequality or the Mermin inequality will be maximized on probability distributions that are algebraically secure. It would be interesting to see, for which correlation inequality this feature holds, and whether it might be possible to find a sufficient criterion to show that the maximal state of a given inequality is algebraically secure.

A. Appendix

A.1. Some facts about C^*- and von Neumann algebras

In this appendix, we summarize some facts about C^* and von Neumann algebras, which will be used to model general quantum systems. For standard textbooks on the subject we refer to e.g. [BR79, BR81, Tak02].

Quantum mechanics of general systems can be described within the formalism of von Neumann algebras. This mathematical structure was first studied by Murray and von Neumann during the 1930th under the name "operator rings" and are also known as "W^*-algebras". Their motivation was to define a general framework for quantum physics that would retain the interpretation of spectral theory as given in the matrix mechanics defined by Born, Jordan and Heisenberg. It was later realized, that von Neumannn algebras are indeed a special case of C^*-algebras, as defined by Gelfand, Naimark and Segal at the end of the 1940th. For more details on the history, we refer to the first chapter of [BR79]. We will follow the presentation that is common in the literature and first define general C^*-algebras and discuss sone of their properties before specifying von Neumann algebras.

Definition A.1.1. *An algebra $\mathcal{A}$ is called a $*$-algebra, if it has an involution $*$ with $(AB)^* = B^*A^*$, $A^{**} = A$ and $(aA + bB)^* = \overline{a}A^* + \overline{b}B^*$ for $A, B \in \mathcal{A}, a, b \in \mathbb{C}$. An algebra with norm is called a Banach algebra, if it is complete with respect to that norm.*

An algebra is called a C^*-algebra, if it is a Banach $*$-algebra for with for all $A \in \mathcal{A}$ it holds that $||A^*A|| = ||A||^2$.

C^*-algebras provides the necessary structure for the discussion of statistical phenomena. Especially they come with a natural concept of positivity, namely an element $a \in \mathcal{A}$ is called positive ($a \geq 0$), if there exists an operator $B \in \mathcal{A}$ with $A = B^*B$, and strictly positive, if this $B \neq 0$. We call the set of all positive elements $\mathcal{A}_+$ We will here only be interested in unital algebras, i.e., in algebras with contain the identity operator $\mathbb{1}$.

An important role will fall to the dual space of the algebra, denoted by $\mathcal{A}^*$, which consists of all continuous linear functionals on the algebra. An element $\omega \in \mathcal{A}^*$ is called positive, if $\omega(A) \geq 0$ for all $A \in \mathcal{A}_+$. We call such a positive functional a state, if $\omega(\mathbb{1}) = 1$.

Next we will define a characterization of mappings between two C^* algebras. Let $\mathcal{A}_1, \mathcal{A}_2$ be two C^*-algebras. We call a linear mapping $\pi : \mathcal{A}_1 \to \mathcal{A}_2$ a $*$-homomorphism, if $\pi(AB) = \pi(A)\pi(B)$ and $\pi(A^*) = \pi(A)^*$. Observe, that a $*$-homomorphism always maps positive elements to positive elements. Furthermore, any $*$-homomorphism is continuous and it holds $||\pi(A)|| \leq ||A||$ (see 2.3.1 in [BR79]).

Definition A.1.2. *A representation of a C^* algebra $\mathcal{A}$ is a $*$-homomorphism into some $\mathcal{B}(\mathcal{H})$. A representation is called faithful, if it is a $*$-isomorphism, i.e., if $Ker(\pi) = 0$.*

A vector $\Omega \in \mathcal{H}$ is called cyclic for the representation, if lin span$\{A\Omega | A \in \mathcal{A}\}$ is dense in $\mathcal{H}$. Every vector $\Omega \in \mathcal{H}$ defines a linear functional on $\mathcal{A}$ via $\omega(A) = \langle\Omega|\pi(A)\Omega\rangle$. Such a functional is always positive, and if π is non-degenerate, i.e., if $\{\psi|\pi(A)\psi = 0 \forall A \in \mathcal{A}\} = 0$ and $||\Omega|| = 1$ it is a state. States of this form will also be called vector states.

Now we have the necessary tools ready to state an important construction primitive for C^*-algebras, namely the Gelfand-Naimark-Segal (GNS) construction:

Theorem A.1.3. *Let $\mathcal{A}$ be a C^*-algebra and $\omega \in \mathcal{A}^*$ a state. Then there exist a Hilbert space $\mathcal{H}$, a representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ and a cyclic vector Ω such that the collection $(\mathcal{H}, \pi, \Omega)$ is a cyclic representation for $\mathcal{A}$, i.e., $\omega(A) = \langle\Omega|A\Omega\rangle$. This representation is unique up to unitary equivalence.*

The proof for the theorem is constructive and can be found in [BR79].

The special class of C^*-algebras that is important for quantum physics are the von Neumann algebras. We will define a von Neumann algebra by its bi-commutant.

Definition A.1.4. *For $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ we denote by $\mathcal{M}'$ the commutant of $\mathcal{M}$, i.e.,$\mathcal{M}' = \{B \in \mathcal{B}(\mathcal{H}) | [A, B] = 0 \forall A \in \mathcal{M}\}$.*
An algebra $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ is called a von Neumann algebra, if

$$\mathcal{M}'' = \mathcal{M}. \tag{A.1}$$

An important property of von Neumann algebras is, that they are closed in different topologies. This property can also be seen as an equivalent definition.

Definition A.1.5. *Let $\mathcal{H}$ be a Hilbert space, $\mathcal{M} \subset \mathcal{H}$.*

- *The map $A \in \mathcal{M} \to |\langle\omega||A\omega\rangle|$ defines a seminorm on $\mathcal{B}(\mathcal{H})$ for any $\Omega \in \mathcal{H}$. The topology induced by these seminorms is called the weak topology.*
- *For any trace class operator $\omega \in \mathcal{M}^*$ the map $A \in \mathcal{M} \to |\omega(A)|$ defines a seminorm on $\mathcal{B}(\mathcal{H})$. The topology induced by these seminorms is called the weak$*$ topology.*
- *The map $A \in \mathcal{M} \to ||A\Omega||$ defines a seminorm on $\mathcal{B}(\mathcal{H})$ for any $\Omega \in \mathcal{H}$. The topology induced by these seminorms is called the strong topology.*

- *For any collection of operators* $\Omega_k, \sum_k ||\Omega_k|| < \infty$ *the map* $A \in \mathcal{M} \to ||\sum_k A\Omega_k||$ *defines a seminorm on* $\mathcal{B}(\mathcal{H})$. *The topology induced by these seminorms is called the strong* topology.*

Theorem A.1.6. *Let* $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ *contain the identity. Then the following conditions are equivalent:*

- $\mathcal{M}'' = \mathcal{M}$.
- $\mathcal{M}$ *is weakly closed.*
- $\mathcal{M}$ *is weakly* closed.*
- $\mathcal{M}$ *is strongly closed.*
- $\mathcal{M}$ *is strongly* closed.*

A.2. Distance measures on the state space

We are often interested to compare quantum systems and to decide, if they are similar, the sense that they show a similar behavior. It is clear, that there is no unique measure of closeness in this sense, but that there are many candidates, in which respect this closeness could be quantified. In this work we are particularly interested in two distance measures, given their operational meaning - the trace distance and the (generalized) fidelity. In the following, we will give the definition for these quantities and their operational meaning for both finite dimensional and general quantum systems. Basic definitions of the quantities are part of the standard textbook material, e.g. Chapter 9 in [NC00]. Applications to smooth entropies can be found in [TCR10, Tom12] for the finite dimensional and [BFS11] for the infinite dimensional case.

We first note the standard definitions. Let $\mathcal{H}$ be finite dimensional, $\rho, \sigma \in \mathcal{B}(\mathcal{H})$ states. Then the trace distance is defined as $d(\rho,\sigma) = 1/2\mathrm{tr}|\rho - \sigma|$.[1] The trace distance quantifies the distinguishability between the states, i.e., the optimal distinguishing operator between ρ and σ will have success probability $1/2 + d(\rho,\sigma)$.

The second important measure is the fidelity, defined as $F(\rho,\sigma) = ||\sqrt{\rho}\otimes\sqrt{\sigma}||^2$. The fidelity can be reformulated according to Uhmann's theorem as

$$F(\rho,\sigma) = \max_{\phi,\psi} |\langle \phi, \psi \rangle|^2, \tag{A.2}$$

where the maximum is taken over all purifications. An important property of the fidelity is, that it is monotonic under trace non-increasing operations. This means

[1] We note, that depending on the literature, the factor 1/2 might or might not be included in the definition.

that, if T is a trance non-increasing operation, it holds

$$F(T(\rho),T(\sigma)) \geq F(\rho,\sigma). \tag{A.3}$$

From this, we can derive as a distance measure the purified distance $P(\rho,\sigma) = \sqrt{1-F(\rho,\sigma)}$. The name referrers to the fact, that it holds that

$$P(\rho,\sigma) = \min_{\phi,\psi} D(\phi,\psi), \tag{A.4}$$

where the minimization is taken over all purifications of ρ and σ.

Both the purified distance and the trace norm form proper metrics on the state space. They can be estimated via each other according to the following set of inequalities:

$$D(\rho,\sigma) \leq P(\rho,\sigma) \leq \sqrt{2D(\rho,\sigma)}. \tag{A.5}$$

Furthermore, the purified distance inherits the monotonicity from the fidelity, i.e., if T is a trace-non increasing map, then

$$P(T(\rho),T(\sigma)) \leq P(\rho,\sigma). \tag{A.6}$$

We will next show, how to generalize the concept of fidelity to (possibly subnormalized) states on von Neumann algebras. The basic idea here is to extend Uhmann's theorem and use this as a definition. To do this, one uses the concept of projective embedding.

Consider von Neumann algebras $\mathcal{M},\mathcal{N}$. We say that $\mathcal{M}$ has a projective embedding in $\mathcal{N}$, if there exists a projector P, such that $P\mathcal{N}P$ is isomorphic to $\mathcal{M}$. We note here, that using a projective embedding we can interpret the normalizing procedure in a natural way as adding an extra measurement outcome with the interpretation of "no measurement". We can now define the generalized fidelity.

Definition A.2.1. *Let ω,ν be states on the von Neumann algebra $\mathcal{M}$. Then we define the generalized fidelity as*

$$F(\omega,\nu) = \sup_{\mathcal{M}\hookrightarrow\mathcal{N}} \sup_{\pi} |\left\langle \xi_\pi^\omega | \xi_\pi^\nu \right\rangle|^2, \tag{A.7}$$

where the first supremum runs over all projective embeddings and the second runs over all representations such that $\omega(x) = \left\langle \xi_\pi^\omega | x \xi_\pi^\omega \right\rangle$ and likewise $\nu(x) = \left\langle \xi_\pi^\nu | x \xi_\pi^\nu \right\rangle$.

We note, that if $\mathcal{M}$ is a full $\mathcal{B}(\mathcal{H})$, the definition coincides with the definition given above. This is a direct consequence of the monotonicity of the fidelity. Using the generalized fidelity, we can now define the purified distance as $P(\omega,\nu) = \sqrt{1-F(\omega,\nu)}$. The generalized fidelity and purified distance inherit many properties from the finite dimensional case, especially the monotonicity holds:

Corollary A.2.2. *Let T be a completely positive contraction, ω,ν states on the von Neumann algebra $\mathcal{M}$. Then it holds*

$$P(T(\omega),T(\nu)) \leq P(\omega,\nu) \quad \textit{and} \quad F(T(\omega),T(\nu)) \geq F(\omega,\nu). \tag{A.8}$$

A.3. The Rényi entropy

We will summarize some fact about the Rényi entropy. For further reference and proofs we refer to [Tom12] and references therein.

Definition A.3.1. *The Rényi entropy of order $\alpha \geq 0$ a classical probability distribution X is defined as*

$$H_\alpha(X) = \frac{1}{1-\alpha} \log \left(\sum_{i=1}^{|X|} p_x^\alpha \right). \tag{A.9}$$

The cases $\alpha = \{0, 1, \infty\}$ are defined via the appropriate limits and can be rewritten as:

$$\begin{aligned} H_0(X) &= \log|X|, & \text{(A.10)} \\ H_1(X) &= H(X), & \text{(A.11)} \\ H_\infty(X) &= \min_x -\log|p_x|. & \text{(A.12)} \end{aligned}$$

The Rényi entropy of order $1/2$ is called max-entropy, the entropy of order 2 is called collision entropy and the entropy of order ∞ is called min-entropy.

Definition A.3.2. *The quantum Rényi entropy of order α of a state ρ is defined as*

$$H_\alpha(\rho) = \frac{1}{1-\alpha} \log \left(tr(\rho)^\alpha \right), \tag{A.13}$$

where the appropriate limits are defined accordingly.

Theorem A.3.3. *The α Rényi entropies obey*

$$H_0 \geq H_\alpha \geq H_\beta \geq H_\infty, \quad \forall \alpha \leq \beta. \tag{A.14}$$

Danksagung

Abschließend möchte ich noch einer Reihe von Menschen danken, die für die Entstehung dieser Arbeit wichtig waren.

Zuerst möchte ich mich bei meinem Chef Reinhard Werner dafür bedanken dass ich so viel von ihm lernen durfte, und dass er mich immer bei allen Projekten unterstützt hat.

Ich danke Andreas Ruschhaupt für die freundliche Übernahme des Korreferats. Ernst Rasel danke ich, dass er meiner Prüfungskommission vorgesessen hat.

Ich hatte das große Glück, beim Verfassen dieser Arbeit nicht nur mit Kollegen, sondern mit guten Freunden zusammen arbeiten zu können. Ich danke vor allem Jörg, Fabian, Vitus und Sönke für Alles was wir zusammen auf die Beine gestellt haben - theoretisch und anderweitig.

Ich danke meinen Koautoren Volkher Scholz, Mario Berta, Marco Tomamichel und Anthony Leverrier auf Seite der Theorie, sowie Roman Schnabel, Tobias Eberle, Aiko Samblowski und Sebastian Steinlechner auf Seite des Experiments.

Mein Dank gilt dem ganzen ITP für die großartige Arbeitsatmosphäre, und natürlich all meinen Kollegen, darunter Kais Abdelkhalek, Andre Ahlbrecht, Mick Bremner, Christopher Cedzich, David Gross, Johannes Gütschow, Sarah Harrison-Schmidt, Jukka Kiukas, Robert Matjeschk Vincent Nesme, Tobias Osborne, Florian Richter, Roland Rüdiger, Rene Schwonnek, Fabian Transchel, Friederike Trimborn, Albert Werner und Wiebke Möller. Für gute Zusammenarbeit in der Anfangszeit der Promotion geht Dank an Annette Gattner, Holger Vogts und Conny Schmidt sowie Stefan Kück.

Für die Zeit in Hannover bedanke ich mich bei Christian, Vanessa und Dominik, sowie für langjährige Freundschaften bei Christoph, Tim, Maik und Friso.

Schließlich danke ich natürlich meinen Eltern, meiner Familie und Christina.

Bibliography

[ABB+10] M.L. Almeida, J.-D. Bancal, N. Brunner, A. Acín, N. Gisin, and S. Pironio. Guess your neighbor's input: A multipartite nonlocal game with no quantum advantage. *Phys. Rev. Lett.*, 104:230404, 2010.

[ABG+07] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007.

[AGR82] A. Aspect, P. Grangier, and G. Roger. Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A New Violation of Bell's Inequalities. *Phys. Rev. Lett.*, 49:91, 1982.

[AGT06] A. Acín, N. Gisin, and B. Toner. Grothendieck's constant and local models for noisy entangled quantum states. *Phys. Rev. A*, 73:062105, 2006.

[BA57] D. Bohm and Y. Aharonov. Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky. *Phys. Rev.*, 108:1070, 1957.

[Bal98] L.E. Ballentine. *Quantum Mechanics: A modern development*. World Schientific Publishing, 1998.

[Bar02] J. Barrett. Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality. *Phys. Rev. A*, 65:042302, 2002.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, page 175, 1984.

[BBB+92] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3, 1992.

[BBCM95] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915, 1995.

[BBM92] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557, 1992.

[BBR88] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210, 1988.

[BCW+12] C. Branciard, E.G. Cavalcanti, S.P. Walborn, V. Scarani, and H.M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85:010301, 2012.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195, 1964.

[Bel87] J.S. Bell. *Speakable and unspeakable in quantum mechanics*. Cambridge University Press, 1987.

[BFS11] M. Berta, F. Furrer, and V. B. Scholz. The Smooth Entropy Formalism on von Neumann Algebras. *arXiv:1107.5460v1*, 2011.

[BHK05] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, 2005.

[BLM+05] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, 71:022101, 2005.

[Boh51] D. Bohm. *Quantum Theory*. Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1951.

[Bor69] M. Born. *Albert Einstein, Max Born: BriefWechsel 1916-1955*. Nymphenburger Verlagshandlung, München, 1969.

[BR79] O. Bratteli and D. W. Robinson. *Operator Algebras and Quantum Statistical Mechanics 1*. Springer, Berlin-Heidelberg-New York, 1979.

[BR81] O. Bratteli and D. W. Robinson. *Operator Algebras and Quantum Statistical Mechanics 2*. Springer, Berlin-Heidelberg-New York, 1981.

[CHRW11] E. G. Cavalcanti, Q. Y. He, M. D. Reid, and H. M. Wiseman. Unified criteria for multipartite quantum nonlocality. *Phys. Rev. A*, 84:032115, 2011.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880, 1969.

[CJWR09] E.G. Cavalcanti, S.J. Jones, H.M. Wiseman, and M.D. Reid. Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. A*, 80:032112, 2009.

[CKMR07] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-half quantum de Finetti theorems. *Comm. Math. Phys.*, 273:473, 2007.

[CKR09] M. Christandl, R. König, and R. Renner. Post-selection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, 2009.

[CLA01] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, 2001.

[CW79] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143, 1979.

[DFSW10a] J. Duhme, T. Franz, S. Schmidt, and R.F. Werner. Quanteninformationstheorie Teil 1: Grundlagen; Verschränkung - Schlüssel zur Quantenwelt. *Physik in unserer Zeit*, 41(5):236, 2010.

[DFSW10b] J. Duhme, T. Franz, S. Schmidt, and R.F. Werner. Quanteninformationstheorie Teil 2: Anwendungen; Geheime Nachrichten und schnelle Rechner. *Physik in unserer Zeit*, 41(6):292, 2010.

[DLTW08] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner. The quantum moment problem and bounds on entangled multi-prover games. *Proceedings of IEEE Conference on Computational Complexity 2008*, page 199, 2008.

[DW03] I. Devetak and A. Winter. Classical data compression with quantum side information. *Phys. Rev. A*, 68(4):042301, 2003.

[DW05] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum state. *Proceedings of Royal Society A*, 461:207, 2005.

[EHD+11a] T. Eberle, V. Händchen, J. Duhme, T. Franz, R.F. Werner, and R. Schnabel. Gaussian entanglement for quantum key distribution from a single-mode squeezing source. *arXiv:1110.3977*, 2011.

[EHD+11b] T. Eberle, V. Händchen, J. Duhme, T. Franz, R.F. Werner, and R. Schnabel. Strong Einstein-Podolsky-Rosen entanglement from a single squeezed light source. *Phys. Rev. A*, 83:052329, 2011.

[Ein07] A. Einstein. Die Plancksche Theorie der Strahlung und die Theorie der spezifischen Wärme. *Annalen der Physik*, 22:180, 1907.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[FAR11] F. Furrer, J. Aberg, and R. Renner. Min- and max-entropy in infinite dimensions. *Comm. Math. Phys.*, 306(1):165, 2011.

[FFB+12] F. Furrer, T. Franz, M. Berta, A. Leverrier, V.B. Scholz, M. Tomamichel, and R.F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.*, 109:100502, 2012.

[FFW11] T. Franz, F. Furrer, and R. F. Werner. Extremal Quantum Correlations and Cryptographic Security. *Phys. Rev. Lett.*, 106:250502, 2011.

[FHD+06] A. Franzen, B. Hage, J. DiGuglielmo, J. Fiurášek, and R. Schnabel. Experimental demonstration of continuous variable purification of squeezed states. *Phys. Rev. Lett.*, 97:150505, 2006.

[Fin82] A. Fine. Hidden variables, joint probability, and the Bell inequalities. *Phys. Rev. Lett.*, 48:291, 1982.

[Fur36] W. H. Furry. Note on the quantum-mechanical theory of measurement. *Phys. Rev.*, 49:393, 1936.

[Fur09] F. Furrer. Min- and max-entropies as generalized entropy measures in infinite-dimensional quantum systems. Master's thesis, ETH Zürich, 2009.

[Fur12] F. Furrer. *Security of Continuous-Variable Quantum Key Distribution and Aspects of Device-Independent Security*. PhD thesis, Leibniz Universität Hannover, 2012.

[FWN+10] M. Fürst, H. Weier, S. Nauerth, D.G. Marangon, C. Kurtsiefer, and H. Weinfurter. High speed optical quantum random number generation. *Opt. Express*, 18(12):13029, 2010.

[GG02] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, 2002.

[GN93] P. Gemmell and N. Naor. Codes for interactive authentication. In *Advances in Cryptology CRYPTO 93*, volume 773 of *Lecture Notes in Computer Science*, page 355. Springer, 1993.

[GP01] D. Gottesman and J. Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, 2001.

[GPC06] R. García-Patrón and N. J. Cerf. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 97:190503, 2006.

[Haa92] R. Haag. *Local Quantum Physics: Fields, Particles, Algebras.* Springer, Berlin, 1992.

[Hän10] E. Hänggi. *Device-independent quantum key distribution.* PhD thesis, ETH Zurich, 2010.

[HES+12] V. Händchen, T. Eberle, S. Steinlechner, A. Samblowski, T. Franz, R.F. Werner, and R. Schnabel. Observation of one-way Einstein-Podolsky-Rosen steering. *Nature Photonics*, 6:598, 2012.

[HOSW84] M. Hilery, R.F. O'Connell, M.O. Scully, and E.P. Wigner. Distribution functions in physics: fundamentals. *Physics Reports*, 106:121, 1984.

[How95] D. Howard. Revisiting the Einstein-Bohr Dialogue. In *Iyyun, Special issue in honor of Mara Beller*, page 57. Hebrew University of Jerusalem, 1995.

[HR10] E. Hänggi and R. Renner. Device-independent quantum key distribution with commuting measurements. *arXiv:1009.1833*, 2010.

[Hwa03] W.-Yo. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, 2003.

[ILL89] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. *Proceedings of 21st Annual ACM Symposium on Theory of Computing*, page 12, 1989.

[JKJL11] P. Jouguet, S. Kunz-Jacques, and A. Leverrier. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Phys. Rev. A*, 84:062317, 2011.

[JNP+11] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V.B. Scholz, and R.F. Werner. Connes' embedding problem and Tsirelson's problem. *J. Math. Phys.*, 52:012102, 2011.

[KR05] R. König and R. Renner. A de Finetti representation for finite symmetric quantum states. *J. Math. Phys.*, 46:122108, 2005.

[Kra90] H. Kragh. *Quantum Generations: A history of physics in the twentieth century.* Princeton University Press, Priceton New Jearsy, 1990.

[KRS09] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. on Information Theory*, 55(9):4674–4681, 2009.

[Kum08] M. Kumar. *Quantum: Einstein, Bohr and the great debate about the nature of reality*. Icon Books, London, 2008.

[LC99] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050, 1999.

[LGG10] A. Leverrier, F. Grosshans, and P. Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, 2010.

[Lud83] G. Ludwig. *Foundations of Quantum Mechanics*. Springer, New York, 1983.

[Lüt00] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61, 2000.

[Mas03] L. Masanes. Necessary and sufficient condition for quantum-generated correlations. *arXiv:quant-ph/0309137*, 2003.

[Mas05] L. Masanes. Extremal quantum correlations for n parties with two dichotomic observables per site. *arXiv:quant-ph/0512100*, 2005.

[May96] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In Neal Koblitz, editor, *Advances in Cryptology CRYPTO'96*, volume 1109 of *Lecture Notes in Computer Science*, page 343. Springer Berlin / Heidelberg, 1996.

[Mer90] N. D. Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65:1838, 1990.

[MFO10] S.L.W. Midgley, A.J. Ferris, and M.K. Olsen. Asymmetric Gaussian steering: When Alice and Bob disagree. *Phys. Rev. A*, 81:022101, 2010.

[Moy49] J.E Moyal. Quantum mechanics as a statistical theory. *Mathematical Proceedings of the Cambridge Philosophical Society*, 45:99124, 1949.

[MPA11] L. Masanes, S. Pironio, and A. Acin. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2:238, 2011.

[MU88] H. Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60:1103, 1988.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *In FOCS'98: Proceedings of the Symposium on Foundations of Computer Science*, page 503, 1998.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[NGA06] M. Navascués, F. Grosshans, and A. Acín. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.*, 97:190502, 2006.

[NPA08] M. Navascues, S. Pironio, and A. Acin. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10:073013, 2008.

[OPKP92] Z.Y. Ou, S.F. Pereira, H.J. Kimble, and K.C. Peng. Realization of the Einstein-Podolsky-Rosen paradox for continuous variables. *Phys. Rev. Lett.*, 68:3663, 1992.

[Pau02] V. I. Paulsen. *Completely bounded maps and operator algebras*. Cambridge University Press, 2002.

[PBS11] S. Pironio, J-D Bancal, and V. Scarani. Extremal correlations of the tripartite no-signaling polytope. *Journal of Physics A: Mathematical and Theoretical*, 44(6):065303, 2011.

[Ped08] F. Pedrocchi. An infinite dimensional quantum de Finetti theorem: tests of robustness. Master's thesis, ETH Zürich, 2008.

[Per95] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Press, Dordrecht, 1995.

[PLZ06] T. Paterek, W. Laskowski, and M. Zukowski. On series of multiqubit Bell's inequalities. *Mod. Phys. Lett. A.*, 21:111, 2006.

[QIP] Open problems in quantum information, http://itp.uni-hannover.de/iqproblems/1.

[Ral99] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, 1999.

[RC09] R. Renner and J. I. Cirac. De Finetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.*, 102:110504, 2009.

[RDC+09] M.D. Reid, P.D. Drummond, E.G. Cavalcanti, P.K. Lam, H.-A. Bachor, U.L. Andersen, and G. Leuchs. The Einstein-Podolsky-Rosen paradox: From concepts to applications. *Rev. Mod. Phys.*, 81:1727, 2009.

[Rei89] M.D. Reid. Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification. *Phys. Rev. A*, 40:913, 1989.

[Ren05] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, 2005.

[RK05] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. *Springer Lecture Notes in Computer Science*, 3378:407, 2005.

[RR12] J. M. Renes and R. Renner. One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys. *IEEE Transactions on Information Theory*, 58:1985, 2012.

[RS78] M. Reed and B. Simon. *Methods of Modern Mathematical Physics, Vol. I: Functional Analysis*. NewYork Academic Press, 1978.

[RS89] I. Raeburn and A. M. Sinclair. The C*-algebra generated by two projections. *Mathematica Scandenavica*, 65:278, 1989.

[RW05] R. Renner and S. Wolf. Simple and tight bounds for information reconciliation and privacy amplification. *Springer Lecture Notes in Computer Science*, 3788:199, 2005.

[SBES11] S. Steinlechner, J. Bauchrowitz, T. Eberle, and R. Schnabel. Strong EPR-steering with unconditional entangled states. *arXiv:1112.0461*, 2011.

[SBPC+09] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301, 2009.

[Sch35a] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Die Naturwissenschaften*, 48:807, 1935. and 49:823 and 50:844.

[Sch35b] E. Schrödinger. Discussion of Probability Relations between Separated Systems. *Proceedings of the Cambridge Philosophical Society*, 31:555, 1935.

[Sch49] P. Schlipp. *Albert Einstein: Philosopher-Scientist*. Library of Living Philosophers, Evaston, 1949.

[Sch63] E. Schrödinger. *Die Wellenmechanik*. Dokumente der Natrwissenschaft. Ernst Battenberg Verlag, Stuttgart, 1963.

[Ser74] R.J. Serfling. Probability inequalities for the sum in sampling without replacement. *Annals of Statistics*, 2:39, 1974.

[Sim00] R. Simon. Peres-Horodecki separability criterion for continuous variable systems. *Phys. Rev. Lett.*, 84:2726, 2000.

[Sin99] S. Singh. *The code book*. Fourth Estate, London, 1999.

[SP00] P.W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85:441, 2000.

[SRLL02] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous Variable Quantum Cryptography: Beating the 3 db Loss Limit. *Phys. Rev. Lett.*, 89:167901, 2002.

[Sti55] W.F. Stinespring. Positive functions on C*-algebras. *Proc. Amer. Math. Soc.*, 6:211, 1955.

[Sti91] D. R. Stinson. Universal hashing and authentication codes. In *Advances in Cryptology CRYPTO 91*, volume 576 of *Lecture Notes in Computer Science*, page 74. Springer, 1991.

[SW71] D. Slepian and J. Wolf. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, 19:461, 1971.

[SW08] V. B. Scholz and R. F. Werner. Tsirelson's problem. *arXiv:0812.4305v1*, 2008.

[Tak02] M. Takesaki. *Theory of Operator Algebras 1 - 3*. Springer, Berlin Heidelberg New York, 2001-2002.

[TCR09] M. Tomamichel, R. Colbeck, and R. Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, 55:5840, 2009.

[TCR10] M. Tomamichel, R. Colbeck, and R. Renner. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56:4674, 2010.

[TLGR12] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3:634, 2012.

[Tom12] M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. PhD thesis, ETH Zürich, 2012.

[TR11] M. Tomamichel and R. Renner. The uncertainty relation for smooth entropies. *Phys. Rev. Lett.*, 106:110506, 2011.

[Tsi80] B. S. Tsirelson. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4:93, 1980.

[Tsi85] B. S. Tsirel'son. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *Journal of Soviet mathematics*, 36(4):557, 1985.

[TYYF07] Y. Takeno, M. Yukawa, H. Yonezawa, and A. Furusawa. Observation of -9 db quadrature squeezing with improvement of phase stability in homodyne measurement. *Opt. Express*, 15:4321, 2007.

[vAIC05] G. van Assche, S. Iblisdir, and N. J. Cerf. Secure coherent-state quantum key distribution protocols with efficient reconciliation. *Phys. Rev. A*, 71:052304, 2005.

[vdW69] B.L. van der Waerden. *Sources of quantum mechanics*. North-Holland publishing company, 1969.

[Ver01] F. Verstraete. *A study of entanglement in quantum information theory*. PhD thesis, Katholieke Universiteit Leuven, 2001.

[vN32] J. von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Verlag Julius Springer, Berlin, 1932.

[vN49] J. von Neumann. Zur Algebra der Funktionaloperationen und Theorie der normalen Operatoren. *Mathematische Annalen*, 102:370, 1949.

[WC81] M. N. Wegman and J. L. Carter. New hash functions an their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265, 1981.

[Wer89] R.F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277, 1989.

[Wey50] H. Weyl. *The theory of groups and quantum mechanics*. Dover publications, New York, 1950.

[Wie84] S. Wiesner. Conjugate coding. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, page 175, 1984. Originally written c. 1970 but unpublished.

[Wig32] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40:749, 1932.

[WJD07] H.M. Wiseman, S.J. Jones, and A.C. Doherty. Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox. *Phys. Rev. Lett.*, 98:140402, 2007.

[WJD+08] K. Wagner, J. Janousek, V. Delaubert, H. Zou, C. Harb, N. Treps, J.F. Morizur, P.K. Lam, and H.-A. Bachor. Entangling the spatial properties of laser beams. *Science*, 321:541, 2008.

[WM04] D.F. Walls and G.J. Milburn. *Quantum Optics*. Springer Berlin, 2004.

[WPGP+12] C. Weedbrook, S Pirandola, R. García-Patrón, N. Cerf, T.C. Ralph, J.H. Shapiro, and S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621, 2012.

[WW01] R. F. Werner and M. M. Wolf. All multipartite Bell correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64(3):032112, 2001.

Curriculum Vitae

Full name:	Torsten Franz
Date of birth:	21.02.1981
Place of birth:	Braunschweig

Positions and Education

From Dec. 2012	University of Braunschweig Institut für Fachdidaktik der Naturwissenschaften
Apr. 2008 - Nov. 2012	Leibniz University Hannover Institute for Theoretical Physics
Aug. 2008 - Mar. 2009	University of Braunschweig Institute for Mathematical Physics
Feb. 2007 - Jul. 2008	Physikalisch Technische Bundesanstalt Braunschweig Section 4.1 Optical Technologies
Feb. 2006 - Jan. 2007	University of Braunschweig Institute for Mathematical Physics
2000 - 2005	Studies of Physics at the University of Braunschweig Degree: Physik Diplom (05 Dec. 2005)
2000	Abitur, Hoffmann von Fallersleben Schule Braunschweig